



Release Notes for Cisco CallManager Release 3.3(5)

April 6, 2005

These release notes describe the new features and caveats for Cisco CallManager release 3.3(5).

Before you install Cisco CallManager, Cisco recommends that you review the “[Important Notes](#)” section on [page 18](#) for information about issues that may affect your system.

For a list of the open and resolved caveats for Cisco CallManager release 3.3(5), see “[Resolved Caveats for Cisco CallManager - Release 3.3\(5\)](#)” section on [page 30](#) and “[Open Caveats for Cisco CallManager - Release 3.3\(5\)](#)” section on [page 35](#). Updates for these release notes occur with every maintenance and major release.

To access the documentation suite for voice products, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/>

You can access the latest software upgrades and release notes for Cisco CallManager 3.3 on Cisco Connection Online (CCO) at

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Contents

These release notes discuss the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Compatibility Matrix and Supported Upgrades, page 3](#)
- [Related Documentation, page 4](#)
- [New and Changed Information, page 4](#)
- [Important Notes, page 18](#)
- [End User Notes, page 28](#)
- [Resolved Caveats for Cisco CallManager - Release 3.3\(5\), page 30](#)
- [Open Caveats for Cisco CallManager - Release 3.3\(5\), page 35](#)
- [Documentation Updates, page 50](#)
- [Obtaining Technical Assistance, page 99](#)

Introduction

Cisco CallManager, a network business communication system, provides high-quality telephony over IP networks. Cisco CallManager enables the conversion of conventional, proprietary, circuit-switched PBXs to multiservice, open LAN systems.

System Requirements

Make sure that you install and configure Cisco CallManager release 3.3 on a Cisco Media Convergence Server (MCS).

You may also install Cisco CallManager on a Cisco-approved HP server configuration or a Cisco-approved IBM server configuration.

**Caution**

The installation does not complete if you do not follow the exact configuration.

Access the correct Cisco-approved server configuration for IBM server or HP server at

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html

For system hardware component information and system requirements, refer to *Installing Cisco CallManager Release 3.3*.

Determining the Software Version

To determine the software version of Cisco CallManager 3.3, open Cisco CallManager Administration; then, click **Details** on Cisco CallManager Administration. The following information displays:

- Cisco CallManager System version
- Cisco CallManager Administration version
- Database information and database DLL versions

Compatibility Matrix and Supported Upgrades

You can find the minimum versions with which Cisco CallManager release 3.3(5) has been tested and which previous release of Cisco CallManager has upgrade support at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/cmcomp.htm



Note

Be aware that the release of Cisco IP telephony products does not always coincide with Cisco CallManager releases. If a product proves to be incompatible with Cisco CallManager, you need to wait until a compatible version of the product becomes available before you upgrade to Cisco CallManager release 3.3(5). For the most current compatibility combinations and defects, refer to the documentation that is distributed with the Cisco IP telephony products.

Related Documentation

Refer to the Cisco CallManager Document Guide for a list of documents that are related to Cisco CallManager release 3.3 at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/doc_gd

Along with the documents that are listed in the Cisco CallManager Document Guide, the following list specifies other related documents for Cisco CallManager:

- [Skinny Client Control Protocol Messaging Guide](#)
- [Cisco CallManager Call Detail Record Definition](#)
- [Cisco IP Phone Services Application Development Notes](#)
- [Cisco CallManager 3.3 JTAPI Installation Guide](#)
- [Cisco JTAPI Developer's Guide for Cisco CallManager 3.3\(3\)](#)
- [Cisco CallManager 3.3 TAPI Installation Guide](#)
- [Cisco TAPI Developer's Guide for Cisco CallManager 3.3\(3\)](#)
- [Cisco CallManager Extension Mobility API Developer's Guide](#)
- [System Error Message](#)

New and Changed Information

This following sections describe new features and changes that are pertinent to this release of Cisco CallManager. The sections include configuration tips for the administrator, information about users, and where to find more information.

- [Requirement for Installation of Java Virtual Machine, page 5](#)
- [Operating System Installation Guidelines, page 8](#)
- [Changes to Type-Specific Information in the Gateway Configuration Settings, page 8](#)
- [Forced Authorization Codes and Client Matter Codes, page 9](#)
- [Cisco WebDialer, page 10](#)
- [Cisco IP Telephony Backup and Restore System \(BARS\), page 11](#)

- [New and Updated Phone Support](#), page 11
- [Extension Mobility Enhancements](#), page 12
- [Cisco Security Agent](#), page 14
- [Image Authentication](#), page 14
- [Router-based Conference Capability](#), page 14
- [International Dial Plan](#), page 16
- [Calling Search Space Enhancements](#), page 17
- [Default Trace Level Changed for Cisco Database Layer Monitor Service](#), page 17
- [New Service Parameter to Enable Music On Hold Duplex Streaming](#), page 17

Requirement for Installation of Java Virtual Machine

The Microsoft Java Virtual Machine (MSJVM) technology allows Java applications to run on Microsoft Windows-based computers. Some versions of Microsoft Internet Explorer (a component of the Windows operating systems) included MSJVM, but Microsoft has since discontinued distribution of MSJVM in its software and announced end-of-life support for the product.

MSJVM was installed by default in all client workstation versions of the current Windows operating systems, except for the following versions:

- Windows XP Professional with SP1 slipstreamed into the installation
- Windows 2000 Server/Professional with SP4 slipstreamed into the installation



Note

Because the Cisco CallManager Administration windows depend on remote scripts, which depend on the JVM for web interaction, Cisco CallManager requires the use of JVM on the client machine to ensure that the Cisco CallManager Administration windows display correctly.

- If your client machine runs MSJVM, you can continue to use the existing configuration to browse into the Cisco CallManager Administration windows and perform administration tasks.

- If you do not have MSJVM installed on your client machine (or if you receive an error message stating that Cisco CallManager cannot detect JVM on the client machine), and you need to perform Cisco CallManager Administration tasks, you must install and configure the Sun Microsystems Java Virtual Machine (JVM) on the client machine. (The Sun JVM comprises part of the Java 2 Runtime Environment—JRE.) In addition, you must configure the browser security to be Java-enabled. See the “[JRE Installation](#)” section on [page 6](#) for information about installing JRE on the client machine.
- If you are not sure whether MSJVM is installed on the client machine, you can install the Sun J2RE anyway. You would then have two Java Runtime Environments installed and running on your machine.



Tip

If you run two separate JVM products (MSJVM and Sun J2RE) on your client machine, be sure to download and install patches and security updates for each JVM from the appropriate software vendor (Microsoft and Sun).

JRE Installation

As part of the Cisco CallManager installation, the system provides the Sun JRE client software in a zip file that is installed on the Cisco CallManager server.



Note

Windows XP/XP Professional includes a built-in tool that handles zip files. If you use Windows 2000 as your operating system, you must obtain a separate compression utility (such as WinZip) to store and access zip files.



Tip

Be sure you install Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2-6-sr5 (or later) before you upgrade to Cisco CallManager release 3.3(5).

To install the JRE software on the client PC, follow these steps:

Procedure

-
- Step 1** From the Cisco CallManager server, navigate to the **C:\utils\JRE** directory and search for the **J2RE_Client_<jre version>.zip** file.

The following shows an example of the zip file name:

J2RE_Client_1.4.2_05.zip



Note Only the Cisco CallManager Administrator can access the JRE software on the Cisco CallManager server; to enable access to other users, copy the J2RE_Client_<jre version>.zip file to a server that can be shared by all users.

Step 2 Right-click the **J2RE_Client_<jre version>.zip** file and click **Copy** to copy the file to your client PC.

Step 3 Double-click the **J2RE_Client_<jre version>.zip** file to unzip the Sun J2RE installation executable.

Step 4 Double-click the installation executable file on the client PC.

The following shows an example of the installation executable file name:

j2re-1_4_2_04-windows-i586-p.exe



Note The exact name of the installation executable file changes with each version as the new version number is incorporated into the name.

The JRE software installs in the C:\Program Files\Cisco\Java\JRE directory.



Note Refer to the *Cisco CallManager Compatibility Matrix* for important information about the supported upgrade path for Cisco CallManager release 3.3(5).

For detailed information about installing and upgrading Cisco CallManager release 3.3(5), refer to *Installing Cisco CallManager Release 3.3(5)* and *Upgrading Cisco CallManager 3.3(5)*.

Operating System Installation Guidelines

Ensure that Cisco IP Telephony operating system version 2000.2.6 with the latest service release 2000.2-6-sr5 (or later) is installed before you upgrade to Cisco CallManager release 3.3(5).

Changes to Type-Specific Information in the Gateway Configuration Settings

After you install Cisco CallManager 3.3(5), the system leaves the following check boxes in the Cisco CallManager Administration Gateway Configuration window unchecked by default for some gateways:

- Display IE Delivery
- Redirecting Number IE Delivery-Inbound
- Redirecting Number IE Delivery-Outbound

This setup affects the following gateways:

- Catalyst 6000 T1 VoIP Gateway (Digital Access PRI)
- Catalyst 6000 E1 VoIP Gateway
- DE-30+ Gateway
- DE-24+ Gateway (Digital Access PRI)
- H.323 Gateway

If you upgrade your server to Cisco CallManager 3.3(5) and you did not uncheck the check boxes before the upgrade, the check boxes remain checked after the upgrade. If you add an affected gateway after the upgrade, the check box remains unchecked.

To determine when you should check the check box(es), refer to the guidelines that are specified in the *Cisco CallManager Administration Guide*.

Where to Find More Information

- *Cisco CallManager Administration Guide*

Forced Authorization Codes and Client Matter Codes

Forced Authorization Code (FAC) and Client Matter Code (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while FACs regulate the types of calls that certain users can place.

Client Matter Codes force the user to enter a code to specify that the call relates to a specific client matter. You can assign CMC to customers, students, or other populations for call accounting and billing purposes. The Forced Authorization Code feature forces the user to enter a valid authorization code before the call completes.

The CMC and FAC features require that you make changes to route patterns and perform configuration tasks for CMC and FAC in Cisco CallManager Administration (Choose **Feature > Client Matter Code** or **Feature > Forced Authorization Code**).

You can use BAT to insert, update, and delete CMC and FAC and CDR Analysis and Reporting (CAR) to run reports that provide call details for authorization code names, authorization levels, and CMCs.



Caution

When you enable FAC or CMC in route patterns, applications that do not pass the FAC or CMC code cannot complete a call. The call times out and fails. This affects all applications, such as Cisco Customer Response Solutions (Cisco CRS), that pass calls through a route pattern with FAC or CMC enabled. You must use a route pattern with FAC and CMC disabled or configure the application to pass the applicable FAC or CMC code. Refer to the application's documentation to find out how you can configure your application to support FAC/CMC.



Note

In the Cisco CallManager 3.3(5) release, CTI does not support the tones that are associated with FAC/CMC; that is, if a user places a call through a TAPI or JTAPI application that uses a FAC/CMC-enabled route pattern, the call times out and fails. In addition, while Personal Assistant 1.4(5) is supported for use with Cisco CallManager 3.3(5), it does not support FAC/CMC in this release because CTI does not support the associated tones. Cisco strongly recommends that you do not configure FAC/CMC-enabled route patterns for any 3.3(5) compatible TAPI or JTAPI application, including Cisco-supported or Cisco-approved, third-party applications (for example, IVR, and SoftPhone.).

How This Feature Affects the User

When enabled, these features force the user to enter a valid account code or authorization code before the call completes. A distinctive tone prompts the user.

You should tell affected end users how to recognize the audio prompts and the codes that users need to enter as well as the consequences or symptoms that are associated with failing to enter a valid code.

Currently, the end-user documentation does not contain any instructions about how to use these features.

Where to Find More Information

- *Cisco CallManager Features and Services Guide*
- *Bulk Administration Tool User Guide*
- *Cisco CallManager Serviceability Administration Guide*
- *Cisco CallManager Serviceability System Guide.*

Cisco WebDialer

Cisco WebDialer allows Cisco IP Phone users to make telephone calls by using web and desktop applications. When you enable your company directory search page by using Cisco WebDialer, a user can make calls by clicking a hyperlinked telephone number.

In Cisco CallManager 3.3(3), users obtain Cisco WebDialer as a download from www.cisco.com. In Cisco CallManager 3.3(5), Cisco WebDialer exists as a service in Cisco CallManager Serviceability.

How This Feature Affects the User

Some current versions of model-specific user guides do not mention Cisco WebDialer features, even though the phone supports these features and the feature might be accessible to end users. Refer users to *Customizing Your Cisco IP Phone on the Web* for instructions about using these features.

Where to Find More Information

- *Cisco CallManager Features and Services Guide*

Cisco IP Telephony Backup and Restore System (BARS)

Cisco CallManager 3.3(5) uses the Cisco IP Telephony Backup and Restore System (BARS) for backup and restore operations, including backing up data, restoring data, and restoring servers. This application, which you can use for manual or scheduled backups, supports compatible versions of Cisco CallManager, Cisco Emergency Responder, Cisco Customer Response Applications/Solutions (CRA/CRS), and Cisco CDR Analysis and Reporting (CAR).

Where to Find More Information

- *Cisco CallManager Compatibility Matrix* to identify which version of BARS supports this version of Cisco CallManager
- Cisco IP Telephony Backup and Restore System (BARS) documentation that supports this version of Cisco CallManager.

New and Updated Phone Support

The following information describes new and updated phone support for this Cisco CallManager release. The applicable documentation may not provide the following information:

- Cisco CallManager release 3.3(5) includes support for Cisco IP Conference Station 7936, Cisco Wireless IP Phone 7920, and Cisco IP Phone model 7970.
- Cisco CallManager 3.3(5) supports Cisco IP Communicator, a Skinny Client Control Protocol (SCCP) based desktop application that turns your computer into a full-featured Cisco IP Phone.
- Cisco CallManager Attendant Console supports Cisco IP Phone models 7902, 7905, 7912, 7940, 7960, and 7970.
- Cisco CallManager allows you to tighten security on certain phones by disabling phone settings in Cisco CallManager Administration.
- Cisco CallManager supports phone image authentication. To identify which phones support image authentication, see [“Image Authentication” section on page 14](#).

Where to Find More Information

- *Cisco IP Conference Station 7936 Administration Guide*
- *Cisco Wireless IP Phone 7920 Administrator Guide*
- *Cisco IP Phone 7970 Administration Guide for Cisco CallManager*
- *Cisco IP Communicator Administration Guide*
- *Cisco CallManager System Guide*

Extension Mobility Enhancements

Cisco CallManager 3.3(5) includes the following enhancements to Extension Mobility.

IP Phone Support

Cisco CallManager 3.3(5) extends Cisco CallManager Extension Mobility functionality to Cisco IP Phones 7905, 7912, 7970, and Cisco IP Communicator.

How This Feature Affects the User

Some current versions of model-specific user guides do not mention Cisco Extension Mobility, even though the phone supports these features and the features may be accessible to end users. Refer users to *Customizing Your Cisco IP Phone on the Web* for instructions about using these features.

Changes to Support MSJVM Removal

Cisco CallManager 3.3(5) includes the following changes to Extension Mobility in support of the MSJVM dependency removal. (See the [“Requirement for Installation of Java Virtual Machine”](#) section on page 5 for more information about MSJVM.)

- The Extension Mobility Logout Service has been removed as an NT Service from the Cisco CallManager Serviceability window.
- The Cisco Extension Mobility service now runs as an application on the Cisco Tomcat Web Service. (As an NT service, Cisco Tomcat installs with Cisco CallManager and loads Cisco CallManager Extension Mobility on all Cisco CallManager servers in the cluster.)

- To disable the Cisco Extension Mobility service on any node, you must deactivate the Cisco Extension Mobility service from the Cisco CallManager Serviceability Activation Center window; then, you must restart the Cisco Tomcat Web Service for the changes to take effect.
- To start or stop the Cisco Extension Mobility service, use administrative privileges to log in to the Tomcat Manager window by accessing the following URL:

`http://<Cisco Extension Mobility server>/manager/list`

where:

Cisco Extension Mobility server specifies the IP address of the server that has the Cisco Extension Mobility service running on it.



Note Make sure that you restart the Cisco Tomcat Web Service after you make any changes to service activation/deactivation; restarting the Cisco Tomcat Web Service is necessary for changes to take effect.

- Cisco CallManager 3.3(5) removes the following Extension Mobility service parameters from the Cisco CallManager Administration window:

- “Login Service Enabled”

To disable Extension Mobility, you must deactivate the Cisco Extension Mobility service from the Cisco CallManager Serviceability Service Activation window; then, restart the Cisco Tomcat Web Service for the changes to take effect.

- “The 7940 Phone Template for Login”

This parameter defined the template to use when a user logged into a Cisco IP Phone 7940; the system no longer requires this parameter for logins.



Note When you perform configuration changes to Extension Mobility service parameters, a message displays that instructs you to restart the Cisco Tomcat Web Service on all Cisco CallManager servers in the cluster; restarting the Cisco Tomcat Web Service is necessary for the changes to take effect.

Where to Find More Information

For additional information, refer to the Cisco CallManager Extension Mobility chapter in the *Cisco CallManager Features and Services Guide*.

Cisco Security Agent

Cisco CallManager 3.3(5) supports Cisco Security Agent with specific Cisco CallManager profiles. Cisco Security Agent provides host intrusion detection capability on Cisco CallManager servers.

Where to Find More Information

- *Cisco CallManager Compatibility Matrix* to identify which version of Cisco Security Agent supports this version of Cisco CallManager

Image Authentication

Image authentication prevents tampering with the binary image; that is, the firmware load, prior to loading it on the phone. Tampering with the image causes the phone to fail the authentication process and reject the image. Image authentication occurs through signed binary files that are automatically installed with this version of Cisco CallManager. Likewise, firmware updates that you download from cisco.com also provide signed binary images.

Cisco IP Phone models 7970, 7960, 7940, 7912, 7910, 7905G, and 7902G support image authentication with Cisco CallManager release 3.3(5).

Router-based Conference Capability

The Cisco 1700, Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 series voice gateway routers provide conferencing capabilities for Cisco CallManager. These routers provide the following features:

- Cisco Conferencing and Transcoding for Voice Gateway Routers by using the NM-HDV or NM-HDV-FARM network modules. This feature supports up to six parties in a conference.

- Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers by using the Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or by using the NM-HD or NM-HDV2 network modules. This feature supports eight parties in a conference.

**Note**

For more information about these conferencing routers, refer to the IOS router documentation that you received with your router.

Router-enabled conferencing provides the capability to support voice conferences in hardware. Digital Signaling Processors (DSPs) convert multiple Voice over IP media streams into time-division multiplexing (TDM) streams that are mixed into a single conference call stream. The DSPs support both Meet-me and ad hoc conferences by Cisco CallManager.

The Cisco routers that support conferencing provide support for the following codecs:

- G.711 a/u-law
- G.729, G.729a, G.729b, G.729ab
- GSM Full Rate (FR), GSM Enhanced Full Rate (EFR) (only supports Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers feature)

Conference Bridge Types for Router Based Conferences

Cisco IOS Conferencing and Transcoding for Voice Gateway Routers

The Cisco IOS Conferencing and Transcoding for Voice Gateway Routers feature uses the NM-HDV or NM-HDV-FARM network modules. This feature enables G.711, G.729, G.729a, G.729b, G.729ab participants to join in a single conference and it provides support for up to six parties in a single conference call.

- Cisco CallManager assigns conference resources to calls on a dynamic basis.
- In a Cisco CallManager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, configure the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum Meetme Conference Unicast, to six conference participants.

Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers

The Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers feature uses the onboard Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or the NM-HD or NM-HDV2 network modules.

This feature enables G.711 a/u-law, G.729, G.729a, G.729b, G.729ab, GSM FR, and GSM EFR participants to join in a single conference and it provides support for up to eight parties in a single call.

- Cisco CallManager assigns conference resources to calls on a dynamic basis.
- In a Cisco CallManager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, configure the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum Meetme Conference Unicast, to six conference participants.



Tip

In Cisco CallManager Administration, ensure that you configure the same conference bridge name that exists in the gateway Command Line Interface (CLI). For specific information about configuring conference bridges and transcoders in Cisco CallManager Administration, refer to the *Cisco CallManager Administration Guide*.

For more information about Cisco IOS Conferencing and Transcoding for Voice Gateway Routers or Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers, refer to the IOS documentation that you received with your router.

International Dial Plan

Cisco CallManager International Dial Plan provides country-specific dialing functionality for countries outside the North American Numbering Plan (NANP). The international dial plan includes route pattern wildcards, special characters, calling party transformation settings, and called party transformation settings that non-NANP dial plans use. It also describes the Discard Digit Instructions (DDIs) and tags that dial plans of specific countries use. Cisco CallManager currently supports international dial plans for Japan, the Netherlands, and Portugal.

Where to Find More Information

- *Cisco CallManager International Dial Plan Deployment Guide.*

Calling Search Space Enhancements

Cisco CallManager 3.3(5) provides database enhancements for Calling Search Spaces, so you can make updates to Calling Search Spaces during regular business hours. Cisco removed the Restart Devices button from the Calling Search Space Configuration window in Cisco CallManager Administration because you do not need to restart the associated devices after you update a calling search space. To save your updates, remember to click **Update** after you make changes.

Default Trace Level Changed for Cisco Database Layer Monitor Service

In Cisco CallManager 3.3(5), the default trace level for the Cisco Database Layer Monitor service changed from Error to Significant.

If you change the default trace level before you upgrade the cluster to Cisco CallManager 3.3(5), your setting does not change after the upgrade. If you do not change the default trace level before the upgrade, the setting changes to Significant.

New Service Parameter to Enable Music On Hold Duplex Streaming

Cisco CallManager 3.3(5) introduces a new service parameter, Duplex Streaming Enabled, for music on hold (MOH). This service parameter determines whether MOH uses duplex (two-way) or simplex (one-way) audio streams.

You can configure one of the following values for this service parameter:

- **True**—Set this parameter to True to set up the connection for duplex streaming media when using MOH. Because certain firewalls and NAT devices require duplex audio streams, this option facilitates interoperability with these products.

- False—Set this parameter to False to set up the connection for simplex streaming media when using MOH. The default value specifies False.

Set the Duplex Streaming Enabled service parameter by using Cisco CallManager Administration to access the service parameters (**Service > Service Parameters**). Choose the server where the Cisco CallManager application resides. On the Cisco CallManager Service Parameters Configuration window, scroll down to the **Cluserwide Parameters (Service)** section to configure the Duplex Streaming Enabled parameter.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg49352>.

For detailed information about configuring service parameters, refer to the *Cisco CallManager Administration Guide*.

Important Notes

The following section contains important information that may not have been available in the initial release of documentation for Cisco CallManager release 3.3(5), and includes the following topics:

- [Application Error During an Upgrade, page 19](#)
- [Adding Cisco CallManager Servers, page 19](#)
- [Using the Ping Command During Installation, page 20](#)
- [Locale Installer for Cisco CallManager Release 3.3\(5\), page 20](#)
- [MLA for Cisco CallManager 3.3\(5\), page 21](#)
- [Cisco CallManager Renamed After Restarting Services, page 21](#)
- [VirusScan on Cisco CallManager Servers, page 22](#)
- [Region Configuration, page 22](#)
- [QSIG Support, page 22](#)
- [Supported Characters in the Directory, page 22](#)
- [Cisco CallManager Integration with Corporate Directories, page 23](#)
- [Installing IPMA Assistant Console on Microsoft Windows XP, page 23](#)
- [Cisco VG248 Analog Phone Gateway \(VG248\) Support, page 24](#)

- [Changing User IDs, page 24](#)
- [Settings Access on Cisco IP Phone 7940/7960, page 24](#)
- [Cisco CallManager Attendant Console Support, page 25](#)
- [Changing the Attendant Console Password, page 25](#)
- [Using Cisco CallManager Attendant Console with Windows XP SP2, page 26](#)
- [Upgrading Cisco CallManager Extension Mobility, page 27](#)
- [Adding Cisco CallManager Servers, page 19](#)

Application Error During an Upgrade

When you upgrade to Cisco CallManager 3.3(5), you may encounter the following error message:

InsertCDR.exe – Application Error, The instruction at “0x10250fe7” referenced memory at “0x0000000.” The memory could not be read. Click **OK** to terminate program.

You should click **OK** to exit the dialog box and to continue with the installation of Cisco CallManager 3.3(5). Clicking OK does not terminate your installation; in fact, clicking OK will allow you to successfully upgrade your Cisco CallManager system.

Adding Cisco CallManager Servers

In Cisco CallManager Administration, make sure that you add each server only once on the Server Configuration window (**System > Server**). If you add a server by using the host name and add the same server by using the IP address, Cisco CallManager cannot accurately determine component versions for the server after a Cisco CallManager upgrade. If you have two entries in Cisco CallManager Administration for the same server, delete one of the entries before you upgrade.

Using the Ping Command During Installation

The publisher database server serves as the master database for all servers in the cluster. All servers except the publishing database server maintain subscriber databases, which are copies of the publisher database server.

If you are configuring a subscriber database server, make sure that the server that you are installing can connect to the publishing database server before you begin the installation. The installation process necessitates this connection, so the publisher database server can be copied to the local drive on the subscriber server.

To make sure that a good connection exists between the servers, issue a ping command from the subscriber server to the publisher database server before you try to authenticate to it. Use only a hostname (for example, hostname.cisco.com) with the ping command. If the ping command is not successful, you must exit the installation program, fix the problem, and begin the installation process again.

Locale Installer for Cisco CallManager Release 3.3(5)

For optimal performance, be sure that you use Cisco IP Telephony Locale Installer version 3.3(5) with Cisco CallManager release 3.3(5).



Note

Be aware that all phrases may not display in the desired locale when you install this version of Locale Installer on a system that is running anything other than Cisco CallManager 3.3(5); that is Cisco CallManager 3.3(5) SR(x) and later or Cisco CallManager 3.3(4) SR(x) and earlier.

Refer to the readme file that is posted with the Cisco IP Telephony Locale Installer software on <http://www.cisco.com> for the complete list of supported languages. For a list of available locale installers that are supported for use with specific versions of Cisco CallManager, go to the following URL:
<http://www.cisco.com/kobayashi/sw-center/telephony/callmgr/locale-installer.shtml>.

**Tip**

When using locales, Cisco recommends that you wait until the locale installer that specifically supports Cisco CallManager 3.3(5) becomes available before you upgrade your system to this release of Cisco CallManager. Because some incompatibilities may exist between releases, be sure to only use the locale installer that specifically supports your version of Cisco CallManager.

**Note**

Each release of Cisco CallManager may support a different number of locales. The full suite of Locale Installers that work with Cisco CallManager 3.3(5) can be found on <http://www.cisco.com> about 8-10 weeks after the English version becomes available. You can download the Locale Installers for all languages that are supported with Cisco CallManager 3.3 from the following location: <http://www.cisco.com/cgi-bin/tablebuild.pl/callmgr-locale-33>.

MLA for Cisco CallManager 3.3(5)

To maintain full multilevel administration access functionality in Cisco CallManager 3.3(5), you must use Cisco CallManager Multilevel Administration Access, release 1.2(4). If you do not install Cisco MLA 1.2(4), you will only be able to log in to Cisco CallManager Administration with the administrator password.

Cisco CallManager Renamed After Restarting Services

If you deactivate the Cisco CallManager service in Cisco CallManager Serviceability, the Cisco CallManager where you deactivated the service no longer exists in the database. Hence, you cannot choose the Cisco CallManager for configuration operations in Cisco CallManager Administration because it will not display in the graphical user interface (GUI).

If you reactivate the Cisco CallManager service on the Cisco CallManager, the database creates a Cisco CallManager and adds a “CM_” prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager service on a server with an IP address of 172.19.140.180, CM_172.19.140.180 displays in Cisco CallManager Administration. You can choose the new Cisco CallManager in Cisco CallManager Administration.

VirusScan on Cisco CallManager Servers

If you are using Microsoft Windows OS version 2000.2.4SR5 or 2000.2.5 with McAfee Netshield 2000 or McAfee VirusScan Enterprise Edition, you may encounter a problem authenticating to Cisco CallManager Administration or accessing some areas of Cisco CallManager Administration. Cisco CallManager displays an “HTTP Error 500-12 Application Restarting” error message.

To resolve this problem, you will need to upgrade McAfee Netshield and McAfee VirusScan to use VirusScan Engine Version 4.2.60 or later. You can obtain the latest Virus Scan updates from the Network Associates website.

Region Configuration

The Region Configuration window displays an Items per page drop-down list box that allows you to list 10, 20, 50, 100, or All configured regions. If you choose to display 100 or more regions, Cisco CallManager may experience performance degradation.

QSIG Support

Cisco offers support for Q.SIG basic call and ID services for selected MGCP-controlled gateways and for selected PBX. ID services support depends upon the PBX type. You can find a list of compatible gateways for which Cisco CallManager release 3.3(5) has been tested at

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Supported Characters in the Directory



Caution

Using non-ISO-Latin1 characters greater than 127 with DC Directory, Netscape Directory, or Active Directory can cause directory database errors.

Cisco CallManager release 3.3 supports all ISO-Latin1 (ISO-8859-1) characters and all non-ISO-Latin1 characters in the range 0-127 with any directory.

Cisco CallManager only supports ISO-Latin1 and ASCII characters in the User area of Cisco CallManager Administration.

After you download the locale installer, you can display field names in the User area of Cisco CallManager Administration in your chosen language. However, Cisco CallManager only supports ISO-Latin1 (ISO-8859-1) characters and non-ISO-Latin1 characters in the range 0-127 in the fields and in all user accounts and passwords that are needed to access these windows. If a user enters data that is not in the allowed character range, a dialog box displays and states that the user must enter data by using only ISO-Latin1 characters and non-ISO-Latin1 characters in the range 0-127.

CDR Analysis and Reporting (CAR) supports all ISO-Latin1 (ISO-8859-1) characters and non-ISO-Latin1 characters in the range 0-127.

Cisco CallManager Integration with Corporate Directories

If you have integrated Cisco CallManager with Active Directory or Netscape Directory, you must run the Cisco Customer Directory Configuration Plugin that is packaged with this release on all the Cisco CallManager servers in the cluster, beginning with the publisher. You must complete this step after you successfully upgrade your Cisco CallManager server to release 3.3(5).

To ensure that Cisco CallManager can install the latest schema and new configuration information in the directory, you must enter a user who has the rights to update the schema in the Directory Administrator DN.

For more information about installing the Cisco Customer Directory Configuration Plugin, refer to *Installing the Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 3.3*.

Installing IPMA Assistant Console on Microsoft Windows XP

The installation of Assistant Console for IPMA service fails with Internet Explorer 6 on Windows XP because it does not include Microsoft Java Virtual Machine (JVM). (This does not cause a problem if the system has Microsoft Windows XP Service Pack 1 installed.) If the system does not have Microsoft Windows XP Service Pack 1, you can use the Netscape browser or install the Sun Java Virtual Machine plug-in for Internet Explorer from <http://java.sun.com/getjava/download.html>.

After installing the Sun JVM plugin, continue the IPMA assistant console installation from <http://<server>/ma/Install/IPMAConsoleInstallJar.jsp> where <server> represents the IP address of the Cisco CallManager server.

Cisco VG248 Analog Phone Gateway (VG248) Support

When using the VG248 with Cisco CallManager 3.3, add the device as a Cisco VG248 gateway and configure each port as VGC phone model. This consolidates the 48 analog or SMDI ports onto a single device. However, you still must configure these ports in the VG248 interface, and you should not enter any values in the Port Specific fields of the Phone Configuration window. Because these fields are not operational when you are using the VG248 1.2(1) or earlier software, you must configure these settings locally on the VG248.

For details about using the VG248 with this and other Cisco CallManager versions, see the “Configuring VG248 Ports Using Cisco CallManager” in the *Cisco VG248 Analog Phone Gateway Software Configuration Guide* for details:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/apg/vg248/v1_2/sw_conf/index.htm.

To view the latest compatibility information about the VG248 and Cisco CallManager, access the Cisco VG248 Analog Phone Gateway Version Release Notes on www.cisco.com at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/apg/vg248/v1_2/rel_note/vg248rn6.htm.

Changing User IDs

Cisco CallManager does not support changing an existing user ID in the directory. Some applications, such as Cisco IPMA and Extension Mobility, may not function properly if you change the user ID.

Settings Access on Cisco IP Phone 7940/7960

Users cannot access any button settings when you disable Settings Access for an individual Cisco IP Phone. This includes the settings to change the ring type, volume level, and contrast level.

Cisco CallManager Attendant Console Support

Cisco CallManager Administration 3.3(5) provides the Cisco CallManager Attendant Console 1.2(1) plug-in, although Cisco CallManager Administration Guide 3.3(5) and Cisco CallManager System Guide 3.3(5) support Cisco CallManager Attendant Console 1.1(3). To obtain documentation for attendant console 1.2(1), click the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/attendnt/call_att/index.htm.

Changing the Attendant Console Password

After you create the ac user, as described in the *Cisco CallManager Features and Services Guide*, you can change the ac user password, if necessary, by using the following procedure.

Procedure

-
- Step 1** Log into a Cisco CallManager server.
 - Step 2** To display a command prompt, choose **Start > Run** and enter **cmd** in the Run dialog box.
 - Step 3** Change directories by typing **C:\Program Files\Cisco\CallManagerAttendant**.
 - Step 4** Display the ACServer.properties file by entering **notepad etc\ACServer.properties**.
 - Step 5** Find the **JTAPI_PASSWORD=** line in the ACServer.properties file.
 - Step 6** To generate an encrypted copy of your new password, type **bin\acenc.exe password** at the command prompt, where password equals the password you want to use for the ac user.
The utility generates an encrypted password.
 - Step 7** Enter the encrypted password in the **JTAPI_PASSWORD=** line in the ACServer.properties file.
 - Step 8** Save the ACServer.properties file and close the Notepad application.
 - Step 9** From Cisco CallManager Serviceability, restart the Cisco Telephony Call Dispatcher service.

Step 10 Repeat these steps on all Cisco CallManagers in the cluster.

Refer to the Cisco CallManager Attendant Console documentation for additional information.

Using Cisco CallManager Attendant Console with Windows XP SP2

When you start Cisco CallManager Attendant Console for the first time after you install Windows XP SP2, a dialog box displays that indicates that Windows Firewall has blocked some features of the ACClient application. To create an exception in the Windows Firewall, so you can continue using Cisco CallManager Attendant Console, click **Unblock**. The operating system configures the exception automatically.

If you do not click Unblock when you open Cisco CallManager Attendant Console for the first time after you install Windows XP SP2, use the following procedure to create an exception, so you can continue using Cisco CallManager Attendant Console:

Procedure

- Step 1** Choose **Start > Settings > Control Panel > Windows Firewall**.
The Windows Firewall dialog box displays.
- Step 2** Choose the Exceptions tab.
- Step 3** Click the **Add Program** button.
The Add a Program dialog box displays.
- Step 4** Click **Browse**. Navigate to the ACClient.exe file and click **Open**.
The ACClient displays in the application list on the Exceptions tab of the Windows Firewall dialog box.
- Step 5** Click **Edit**.
The Edit a Program dialog box displays.
- Step 6** Click **Change Scope**.

The Change Scope dialog box displays.

- Step 7** Make sure that you choose the **Any computer (including those on the internet)** radio button.
- Step 8** Click **OK** twice.
-

Upgrading Cisco CallManager Extension Mobility

If you run Cisco CallManager Extension Mobility and Cisco CallManager 3.1 or 3.2 before the upgrade, you must perform additional configuration tasks after the upgrade, so Cisco CallManager Extension Mobility runs as expected. For more information about configuration tasks, refer to the Cisco CallManager Extension Mobility upgrade section of the *Cisco CallManager Features and Services Guide for 3.3*.

Adding Cisco CallManager Servers as Members of a Windows Domain

Cisco does not recommend adding Cisco CallManager servers as members of a Microsoft Windows domain. However, if your system architecture is dependent on servers joining a Windows domain, then you must disable the Network Time Protocol (NTP) software that is installed by Cisco CallManager when you add the server as a member of a domain and use Microsoft time service. You must disable the NTP service on every server in your cluster.

**Note**

You must choose to install Cisco CallManager as a server in a workgroup during installation.

**Note**

Do not make any modifications to the installed NTP configuration file (NTP.CONF); otherwise, you may encounter synchronization problems with CDRs, Traces, Event Logging, etc. Cisco does not support any modifications to the installed NTP configuration file.

Follow this procedure to disable the Cisco-installed NTP software on a server:

Procedure

-
- Step 1** Select **Start > Programs > Administrative Tools > Services**.
 - Step 2** Double-click the **Network Time Protocol** service.
 - Step 3** Select **Disabled** in the Startup type field.
 - Step 4** Click **Stop**.
 - Step 5** Click **OK**.
-



Caution

Cisco CallManager will abort the installation process if it detects that the server is in a Windows domain. Therefore, you must first remove the Cisco CallManager server from the Windows domain and add it as a Workgroup member before you can install or upgrade Cisco CallManager on your server.

When you have completed your upgrade and you are adding the server to the Windows domain, you must disable the Cisco-installed NTP services once again.

If you are joining the server to a Microsoft Windows 4.0 domain, you must also perform an additional procedure for synchronizing time. Refer to *How to Synchronize the Time on a Windows 2000-Based Computer in a Windows NT 4.0 Domain* at <http://www.microsoft.com>.

End User Notes

The following section contains important information that affects the end user. Some features affect Cisco IP Phone end users but might not be included in model-specific documentation for the end user. Cisco suggests that you pass the information on to affected end users.

Attendant Console

The following guidelines apply to Attendant Console:

- The attendant console user cannot drag a speed-dial entry onto a call in the Call Details pane.
- The attendant console user cannot rename a speed-dial group from the Edit menu.
- The Call Forward All to the voice mail icon and the Forward All to another directory number icon do not display in the Speed Dial window.

Ring Settings

The Ring Settings window, a feature in the Cisco IP Phone User Options GUI, allows end users to assign distinctive ring tones to their phone line(s) from their computers. Users can access the Ring Settings window from the User Options main menu. The system administrator determines feature availability.

Cisco IPMA

The following guidelines apply to IPMA:

- A Cisco IPMA assistant can support up to 33 proxy lines.
- A Cisco IPMA manager can have up to 10 assistants.

User Login Name and Password

Cisco CallManager supports only ISO-Latin1 (ISO-8859-1) characters and non-ISO-Latin1 characters in the range 0-127 in user login fields. This restriction affects services or applications that retrieve user login data from the Cisco CallManager database (such as the Cisco IP Phones, Cisco User Options, and the Cisco IPMA service).

If a user enters data that is not in the allowed character range, a dialog box displays and states that the user must enter data by using only ISO-Latin1 characters and non-ISO-Latin1 characters in the range 0-127. System administrators can advise end users who encounter this error message to enter a

user name and/or password in only one of the following languages: Danish, Dutch, English, French, German, Italian, Norwegian, Portuguese, Spanish, Swedish, Hungarian, Polish, Greek, or Japanese.

Phone Hardening

Phone hardening options allow you to configure settings that restrict phone features and functionality for security purposes.

As part of phone hardening, you can disable user access to Cisco CallManager User Options and some phone settings (including those settings that are normally accessible via the Settings button). Because disabling access to these features will directly impact end users, you should advise affected users about the restrictions.

For more information about phone hardening, refer to the “Cisco IP Phone” chapter in the *Cisco CallManager System Guide*.

End-user documentation mentions the possibility of restricted access to some settings; however, Cisco suggests that you provide more detailed information to users who are affected by phone hardening.



Note

You configure phone hardening options in the Cisco CallManager Administration Phone Configuration window. Phone hardening configuration options vary by phone model.

Resolved Caveats for Cisco CallManager - Release 3.3(5)

The Cisco CallManager Release Notes no longer list resolved caveats. Instead, you can find the latest resolved caveat information through Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

**Tip**

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

-
- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
Log on with your Cisco.com user ID and password.
- Step 2** Click the **Launch Bug Toolkit** hyperlink.
- Step 3** If you are looking for information about a specific caveat, enter the ID number in the “Enter known bug ID:” field.

To view all caveats for Cisco CallManager, go to the “Search for bugs in other Cisco software and hardware products” section, and enter **Cisco CallManager** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco CallManager**.
- Step 4** Click **Next**. The Cisco CallManager search window displays.
- Step 5** Choose the filters to query for caveats. You can choose any or all of the available options:
- a. Choose the Cisco CallManager version:
 - Choose the major version for the major releases (such as, 4.1, 4.0, 3.3).

A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.

- Choose the revision for more specific information; for example, choosing major version 3.3 and revision version 5 queries for release 3.3(5) caveats.

A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.

- Choose the Features or Components to query; make your selection from the “Available” list and click Add to place your selection in the “Limit search to” list.
 - To query for all Cisco CallManager caveats for a specified release, choose “All Features” in the left window pane.



Note The default value specifies “All Features” and includes all of the items in the left window pane.

- To query only for Cisco CallManager-related caveats, choose “ciscocm;” then click **Add**.
 - To query only for phone caveats, choose “ciscocm-phone;” then click **Add**.
 - To query only for gateway caveats, choose “voice-gateway;” then click **Add**.
- Enter keywords to search for a caveat title and description, if desired.



Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- Choose the Set Advanced Options, including the following items:
 - Bug Severity level—The default specifies 1-3.
 - Bug Status Group—Check the **Fixed** check box for resolved caveats.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.

- e. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.
- You can save your query for future use. See the [“Saving Bug Toolkit Queries” section on page 33](#).



Note

For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

- Step 1** Perform your search for caveats, as described in the [“Using Bug Toolkit” section on page 31](#).
- Step 2** In the search result window, click the **This Search Criteria** button that displays at the bottom of the window.
A new window displays.
- Step 3** In the Name of saved search field, enter a name for the saved search.
- Step 4** Under My Bug Groups, use one of the following options to save your defects in a bug group:
 - Click the **Existing group** radio button and choose an existing group name from the drop-down list box.
 - Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.



Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time a new bug meets the search criteria, it will be added to the group that you chose.

Bug Toolkit saves your bugs and searches, and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

Step 5 Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:

- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
- **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include
 - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
 - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
- **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.

Step 6 To save your changes, click **Save**.

Step 7 A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.



Note For complete Cisco IP Phone firmware release note information, refer to the applicable firmware release notes for your specific model IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/.

Open Caveats for Cisco CallManager - Release 3.3(5)

[Table 1](#) describes possible unexpected behaviors by Cisco CallManager release 3.3(5), sorted by component. Unless otherwise noted, these caveats apply to all Cisco CallManager 3.0 releases up to and including Cisco CallManager release 3.3(5).

**Tip**

For more information about an individual defect, click the associated Identifier in [Table 1](#) to access the online record for that defect, including workarounds.

Understanding the Fixed-in Version and the Integrated-in Fields in the Online Defect Record

When you open the online record for a defect, you may see data in the “First Fixed-in Version” or “Integrated-in” fields. The information that displays in these fields identifies the list of Cisco CallManager interim versions in which the defect was fixed. These interim versions then get integrated into Cisco CallManager releases.

Some more clearly defined versions include identification for Engineering Specials (ES) or Service Releases (SR); for example 03.3(04)ES29 and 04.0(02a)SR1. However, the version information that displays for the Cisco CallManager maintenance releases may not be as clearly identified.

The following examples show how you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Cisco CallManager release that includes that interim version. You can use these examples as guidance to better understand the presentation of information in these fields.

- 003.003(002.079) = Cisco CallManager release 3.3(3)
- 003.003(003.144) = Cisco CallManager release 3.3(4)
- 004.000(000.123) = Cisco CallManager release 4.0(1)
- 004.000(001.008) = Cisco CallManager release 4.0(2)
- 004.001(002.201) = Cisco CallManager release 4.1(3)



Note Because defect status continually changes, be aware that [Table 1](#) reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the [“Using Bug Toolkit” section on page 31](#).



Tip Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online). By using the Bug Toolkit, you can find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than what is reflected in this document. To access the Bug Toolkit, log on to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 1 *Open Caveats for Cisco CallManager Release 3.3(5)*

Identifier	Headline
	Component: BAT
CSCeg73540	The system displays the incorrect status when phones are deleted using a custom file. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg73540
CSCeg74785	The Export View Query Results window incorrectly displays the phones that are associated to a user. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74785
	Component: Callback
CSCee10684	The Callback feature in the German locale displays in English. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee10684
CSCef73201	The Callback message erroneously displays the previously called DN. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef73201
CSCeg41238	When you press the Dial softkey in Callback notification, the system calls the incorrect number/destination. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg41238
CSCin86736	The system sends incorrect Callback notification when the calling party has Callback enabled. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin86736

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
	Component: Call Processing
CSCin18384	<p>Call Processing: The system may not send H.225 disconnect when the IP connection between the originating Cisco Voice Gateway (H.323 endpoint) and Cisco CallManager goes down.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin18384</p>
CSCdx71866	<p>Call Control: When Cisco CallManager processes a call that uses a translation pattern, the trace files do not display information about the translation that occurred on the number.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdx71866</p>
CSCea91106	<p>Call Control: When you add another Cisco CallManager server to a cluster, you must reboot all servers in the cluster in order to make calls from a phone registered to the new server to other phones in the cluster.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea91106</p>
CSCef11036	<p>Call Control: IP Phone does not display Private after consultant-transfer over an intercluster trunk (ICT).</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef11036</p>
CSCeg54086	<p>Call Control: Users sporadically hear busy tones when they access voicemail.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg54086</p>
CSCeg70015	<p>Call Control: Media Resource Group List is assigned at the device pool level, not the device level.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg70015</p>
CSCec62297	<p>Change Notify: The Route Group update process takes 10-11 minutes to complete, which may impact performance.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec62297</p>
CSCef50588	<p>Change Notify: After changing the name of the IP phone directory number (DN) partition, the DNs that are in the changed partition do not forward to the voice-messaging system.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50588</p>

Table 1 ***Open Caveats for Cisco CallManager Release 3.3(5) (continued)***

Identifier	Headline
CSCed58739	Database: Call Forward All (CFwdAll) database update results in a DBL Exception alarm in Syslog. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed58739
CSCee19228	Database: Phones may register and become active without having an assigned DN. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee19228
CSCef36515	Database: When an IP phone that is configured for CFwdAll restarts by a power cycle, the phone loses CFwdAll notification, but CFwdAll continues to work. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef36515
CSCeg72693	Database: Memory corruption for table CiCrCrpTable caused the CCM.exe service to terminate unexpectedly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg72693
CSCee20237	Digit-Analysis: ALARM:DaTimeout errors in the application event viewer should display an explanation and recommended action. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee20237
CSCed43618	Line Control: A Cisco 79xx model IP Phone may not correctly display the status of a shared line after reset. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed43618
CSCef20324	Media Control: Cisco CallManager closes the logical channel in 8 seconds if there is no connection from an MGCP gateway when calling from an H.323 Alarm Server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef20324
CSCef92445	Media Control: CFwdAll to a voice-messaging system fails with a reorder tone when coming from a device on the other side of an ICT. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef92445
CSCeg71188	Media Control: Music on Hold occasionally pauses when a call is connected to NetMeeting. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg71188

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCeg77257	<p>PRI: The DMS-100 protocol does not recognize ISDN Q.931/Q.850 Disconnect Cause Code of 53, which causes the PRI “B” channels to lock up and become unusable.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg77257</p>
CSCea01715	<p>SCCP: Outbound calls from Cisco CallManager may experience one-way audio when calls are placed to certain third-party H.323 gateways because Cisco CallManager includes the incorrect mediaControlChannel address in the Open Logical Channel.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea01715</p>
CSCeg12505	<p>SCCP: Changing the Ring Setting (Phone Active) does not take effect on the IP phone.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg12505</p>
CSCeg64267	<p>SCCP: Unable to transfer calls when toggling between calls on the Cisco IP Phone 7970.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg64267</p>
CSCeg71123	<p>Supplementary Services: Ringback stops when you barge a blind transferred call.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg71123</p>
CSCeg78353	<p>Supplementary Services: Barged call does not end after blind transferred party ring timeout.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg78353</p>
CSCin86739	<p>Supplementary Services: Modified configurations are restored in the CEF trace configuration.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin86739</p>
CSCec50080	<p>System: The system does not always generate an application event log warning when the Cisco CallManager service stops.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec50080</p>
CSCee40188	<p>System: The service needs to update the SCM database with the services on which it depends.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee40188</p>

Table 1 ***Open Caveats for Cisco CallManager Release 3.3(5) (continued)***

Identifier	Headline
CSCdy80350	Unknown: Database changes do not get queued and delivered to clients. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdy80350
CSCed06857	Unknown: Updating a calling search space with a large number of associated devices results in a forward signal storm, which causes delayed dial tone. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed06857
	Component: CCM-Serviceability
CSCeg22809	Running the Trace Collection Tool generates an error message about invalid account credentials. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg22809
	Component: CCM-Service Parameters
CSCeg55103	Some service parameters, such as SDL Trace Data Flags, accept decimal, binary, or hexadecimal numbers. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg55103
	Component: CMCTI
CSCef13510	Transfer request intermittently fails when the application receives the CiscoJtapiException (InvalidStateExceptionImpl) error message. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef13510
	Component: Database
CSCec62896	After the Cisco CallManager Subscriber is removed, the service fails to start and generates the “One service or driver failed to start properly” error message after logon to the Cisco CallManager publisher server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec62896
CSCee69212	SR installation fails to detect a replication error when the Cisco CallManager publisher server is upgraded to 3.3(4)SR1. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee69212
CSCee69769	The <i>Cisco CallManager Administration Guide</i> contains incorrect information about using the RemoveServerFromDB.bat and RemoveSubscription.bat scripts to clean up the database. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee69769

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCee76819	The server reflects missing DBL components after a new Cisco CallManager installation is performed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee76819
CSCef10283	Upon subscriber server reboots, Cisco CallManager, RISDc, and CTI may terminate unexpectedly. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef10283
CSCeg06441	AutoAnswer works with shared lines. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg06441
CSCeg61863	Users cannot log in to the Cisco CallManager User window after an update is made to the user's control device list. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg61863
CSCeg71132	CFwdAll cannot be set or unset from a phone if the DN includes the [^] character. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg71132
	Component: Database Admin
CSCee01733	The display of the Find/List Route Group search window is delayed when the route group is associated with 200 gateways. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee01733
CSCee88794	Calling Search Space does not get created with the IPMA wizard if a partition gets deleted during wizard execution. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee88794
CSCeg00253	The system does not display the “Domain name is not unique” error when the same device name is configured for H.323 gateway/client/CTI port and an MGCP gateway. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg00253
CSCeg03936	The system displays an error message when you try to add a DN as a shared line. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg03936
CSCeg05156	An invalid Authorization Code Name in the Forced Authorization Code Configuration window causes the system to display an incorrect error message about the description field. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg05156

Table 1 ***Open Caveats for Cisco CallManager Release 3.3(5) (continued)***

Identifier	Headline
CSCeg05186	The system does not display any results when a Meet-me number is searched by using the “partition begins with” criteria and without entering any value in the search. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg05186
CSCeg06860	The system does not return any results when you search for a user device profile where the DN is empty. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg06860
CSCeg07738	An incorrect number of associated devices displays when the devices are associated with a user. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07738
CSCeg07903	The system does not display the “No Matching Records” message when you perform a search by using the Find and List Trunks window and you use a search criteria that produces no results. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07903
CSCeg07917	Alignment gets distorted after you search on the user device association window. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg07917
CSCeg08441	HTTP requests for the DeviceListX.asp report times out when more than 5000 phones are configured and/or registered. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg08441
CSCeg11825	When you search for ATA 186/188 by using the Find and List Phones window, the ATA186/188 displays its matching record, but the hyperlink for its associated IP address does not work. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg11825
CSCeg16515	Searching for a call pickup group by using the exactly="" criteria in the Find and List Phones window returns no results for the phone that does not have an assigned DN. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg16515
CSCeg26559	A remote scripting error occurs when the first line on a phone is used as a shared line. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg26559

Table 1 ***Open Caveats for Cisco CallManager Release 3.3(5) (continued)***

Identifier	Headline
CSCeg27056	When you try to add more than 39 devices in to a Media Resource Group, the update fails and the system displays an error message. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg27056
CSCeg42741	The Message Waiting DN window does not include partition and description fields. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg42741
CSCeg42749	The icon for the Cisco Voice Mail port is misplaced in the Find/List window for search-based on Calling Search Spaces. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg42749
CSCeg42799	The search window becomes inactive after search for a non-existent DN. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg42799
CSCeg44975	The voicemail port wizard occasionally fails to delete voicemail ports. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg44975
CSCeg46293	Incorrect information displays on the User Information, Add a New User, and other related windows when they are viewed using the French locale. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg46293
CSCeg51407	The associated PC field in the softphone configuration in the user configuration window should be marked mandatory. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51407
CSCeg52504	The system does not check for duplicate route filter names when the same name is added with a space. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg52504
CSCeg52857	An error displays when you use route filters in a route pattern that contains more than 249 route filters. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg52857
CSCeg54015	An error displays when you click update instead of an updated AutoGenerate Device Profile Page. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg54015

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCeg55074	1700 gateway FXO ports can be configured for different signalling. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg55074
CSCeg55114	Cisco CallManager Administration displays an incorrect description about resetting and restarting IOS gateways in the Gateway Configuration window. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg55114
CSCeg64265	An error may occur when you try to access the global directory from Cisco CallManager Administration if the Windows regional settings are not configured for US English. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg64265
CSCeg67636	When you check the “Check All in Search” check box, the system does not display all devices across multiple search windows. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg67636
CSCeg67814	A blank pop-up message displays when updating the DN window. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg67814
CSCeg68986	When you perform a search by using some wildcard characters on the Extension Mobility User window, the results display all available user device profiles. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg68986
CSCeg69956	The system displays a RemoteScript error if try to add an existing Meet-me number. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg69956
CSCin59391	Cisco CallManager displays gateways that already have associated DNs. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin59391
CSCin62709	The system displays a remote scripting error on updating the Cisco CallManager Subscriber when the Cisco CallManager Publisher is down. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin62709
CSCin64572	The User Configuration window displays the pilot number as the primary extension after the pilot point that is associated with the user is deleted. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin64572

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCin83845	<p>The system displays an error message when a user device profile as a logout profile is created.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin83845</p>
Component: Dialed Number Analyzer	
CSCef62953	<p>You cannot use Dialed Number Analyzer (DNA) after a failed/cancelled uninstall (rollback) procedure.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef62953</p>
CSCeg48785	<p>No icon displays for the Cisco IP Phone 7971 in DNA.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg48785</p>
Component: Directory	
CSCed12260	<p>Database restoration fails after a same server recovery is performed.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed12260</p>
CSCed57970	<p>The readme documentation for DC Directory scripts version 1.05 needs an update to specify the supported Cisco CallManager versions.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed57970</p>
CSCed58020	<p>DC Directory scripts or procedures are not available on CCO for CCM 3.3(3).</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed58020</p>
CSCee49394	<p>DC Directory logs do not contain useful diagnostics information.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee49394</p>
CSCee60351	<p>Beginning with Cisco CallManager 3.3, you cannot get DCD IntegratedInstall as a separate executable.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee60351</p>
CSCef79862	<p>A need exists to provide an option in the CCMPwdChanger tool to automate the resetting of the DeviceAuthorizationRequired flag in the directory.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef79862</p>
Component: Documentation	

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCef37773	The <i>Troubleshooting Guide for Cisco CallManager</i> needs an update to include information about DC Directory issues. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef37773
CSCeg74702	The default value for the maximum number of files on the SDI/SDL help window should reflect 250. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74702
CSCeg74702	The default value for the maximum number of files on the SDI/SDL help window should reflect 250. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74702
Component: ES-SR-Wrapper	
CSCef54820	Incorrect devpack version in Cisco CallManager may allow the installation process to overwrite the newer devpack with the older devpack. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef54820
CSCef60553	Patch install changes the attributes of the files that it replaces to “Read Only.” http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef60553
Component: IPMA Service	
CSCeb31088	Application Error displays after the Cisco CallManager publisher server is upgraded. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb31088
CSCec83549	When you run the IPMA configuration wizard a second time, the wizard displays a blank screen if the status contains longer text. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCec83549
CSCed27237	A search for IPMA assistants times out when Cisco CallManager is integrated with Active Directory if the directory contains a large number of objects. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed27237
CSCed79991	The IPMA status window displays when a new user logs in to the phone. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed79991

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCee73576	<p>The IPMA Manager Configuration window does not function after an invalid character (\) is saved in the Divert Configuration window.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee73576</p>
CSCef61861	<p>The IPMA DND and Intercept softkeys become inactive after Extension Mobility logout.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef61861</p>
CSCeg52533	<p>The assistant page cannot be found if you search for a user that includes special characters.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg52533</p>
CSCeg67858	<p>An incorrect DN displays on the assistant watch window on the manager phone when a transferred call is answered on the assistant phone.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg67858</p>
CSCeg70036	<p>The Cisco Systems copyright information needs to be updated on the IPMA Manager Login window.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg70036</p>
CSCeg76132	<p>The IPMA Assistant Console cannot search the directory for names that contain spaces.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg76132</p>
CSCin84477	<p>After saving an update to the IPMA Manager configuration, the window should return to the same tab after submission.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCin84477</p>
Component: MLA	
CSCeg02724	<p>The system allows a change to the Cisco CallManager Administrator password when the Cisco CallManager publisher server is shut down.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg02724</p>
CSCeg51348	<p>Users cannot move between application and Cisco CallManager Serviceability windows.</p> <p>http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51348</p>

Table 1 *Open Caveats for Cisco CallManager Release 3.3(5) (continued)*

Identifier	Headline
CSCeg51353	FullAccess MLA users cannot delete users. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51353
CSCeg51358	FullAccess MLA users can change the Cisco CallManager administrator password. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51358
CSCeg51374	FullAccess MLA users cannot click the Update and Change buttons after inserting a new user. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51374
CSCeg51389	The “Response.Buffer = true” error displays on the External Route Plan Wizard when you login as Administrator, FullAccess or ReadOnly user. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51389
CSCeg51394	The system displays a “page expired” message when you click the back button in the IE browser. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg51394
	Component: QED
CSCeg38281	No DN displays on a Cisco IP Phone 7971 when the phone auto registers with Cisco CallManager. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg38281
CSCeg39216	For a Cisco IP Phone 7971, JTAPI sends an extra OutofService and Inservice event during Cisco CallManager failover. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg39216
CSCeg43803	Cisco CallManager Administration does not include support for NM-2FE2W_V2 associated AIM (voice) modules. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg43803
	Component: SDL
CSCeg23478	Phones do not display a status of standby for the secondary Cisco CallManager server, and they cannot failover to their backup server. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg23478
	Component: Serv-Web-Pages

Table 1 **Open Caveats for Cisco CallManager Release 3.3(5) (continued)**

Identifier	Headline
CSCeg74691	When you run an SDI Trace, a message should display that shows the allowable maximum number of files. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74691
	Component: TAPISDK
CSCef26258	If you configure a duplicate directory number for multiple lines that are in different or the same Cisco CallManager partition, CTI only sends one instance of the line in response to requests from WebAttendant, ARC Console, and Attendant Console. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef26258
	Component: Upgrade Assistant
CSCeg78327	Upgrade and Upgrade Assistant report different results depending on the version of OS that you have installed. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg78327
CSCed88989	Upgrade Assistant does not use the correct logic when checking the “OS Service Release” key. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed88989
The following firmware caveats apply to this release.	
CSCee27943	SW-6608: Output dB padding does not attenuate relayed DTMF tones. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee27943
CSCef56344	SW-6624: The 6624 phone goes dead when you attempt a hookflash transfer and the call is in a held state. http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef56344

**Note**

For complete Cisco IP Phone firmware release note information, refer to the applicable firmware release notes for your specific model IP phone at http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/.

Documentation Updates

This section provides documentation changes that were unavailable when the Cisco CallManager release 3.3(5) documentation suite was released.

This section contains the following types of updates:

- [Errors, page 50](#)
- [Changes, page 56](#)
- [Omissions, page 61](#)

Errors

This section includes errors that the Cisco CallManager Documentation suite contains and includes the following topics:

- [Locale Installer, page 51](#)
- [Microsoft Outlook Support with Cisco WebDialer, page 51](#)
- [Mandatory Parameter for Cisco WebDialer API Reference, page 51](#)
- [Date/Time Configuration Changes, page 51](#)
- [User Configuration Settings, page 52](#)
- [Using Valid Characters in Cisco CallManager User IDs, page 52](#)
- [Cisco CallManager Dialed Number Analyzer Private Phrase Requirement, page 53](#)
- [Cisco CallManager Dialed Number Analyzer Service Startup Type, page 54](#)
- [Supported Number of Alphanumeric Characters in the AAR Group Name Field, page 54](#)
- [Default Value for the Extension Mobility Alphanumeric Userid Service Parameter, page 54](#)
- [Updated Directory Path for Music On Hold Drop Directory, page 55](#)
- [Default Value for Display IE and Redirecting IE Delivery Fields, page 55](#)
- [Support for Overlap Route Patterns, page 56](#)

Locale Installer

The *Cisco CallManager Documentation Guide for Release 3.3(3)* incorrectly refers to *Using the Cisco IP Telephony Locale Installer for Cisco CallManager 3.3(3)*. The correct document is *Using the Cisco IP Telephony Locale Installer with Cisco CallManager 3.3(3)sr1*.

Microsoft Outlook Support with Cisco WebDialer

The Cisco WebDialer API Reference chapter in the *Cisco WebDialer Guide* states that the makeCallSoap interface (that plug-in clients such as Microsoft Outlook Plug-In use) is accessed by initiating a Simple Object Access Protocol (SOAP) request to a specified URL. The specified URL contains the IP address of the Cisco CallManager server. However, Cisco does not provide a Cisco WebDialer plug-in that works with Microsoft Outlook. If you require this type of plug-in, contact a third-party vendor or partner.

Mandatory Parameter for Cisco WebDialer API Reference

The Cisco WebDialer API Reference chapter in the *Cisco WebDialer Guide* incorrectly specifies a mandatory parameter for the makeCallProxy interface as appuid. The correct parameter to use is appid. This mandatory parameter must properly reflect appid for the Cisco WebDialer API to function correctly.

Date/Time Configuration Changes

The *Cisco CallManager Administration Guide* incorrectly states that the “local time zone of CallManager” option exists in the Date/Time Configuration window, Time Zone parameter. However, the drop-down box in Cisco CallManager 3.3(5) does not offer this option.

If you upgrade from a compatible Cisco CallManager release and you use “local time zone of CallManager” in the configuration, the Cisco CallManager database determines the appropriate time zone for the publisher database server and then displays that time zone as replacement for the CallManager time zone.

If you perform a fresh installation of Cisco CallManager, the default setting for Time Zone in the Date/Time Group equals GMT (Monrovia, Casablanca).

User Configuration Settings

The “Adding A New User” chapter in the *Cisco CallManager Administration Guide* erroneously states that Cisco CallManager does not allow you to use the following special characters in any field in the User Information window: =, +, <, >, #, ;, \, , , “”, and blank spaces.

This information is not correct; Cisco CallManager does allow input of special characters in the First Name, Last Name, UserID, and User Password fields in the User Configuration Settings.

The “Adding A New User” chapter in the *Cisco CallManager Administration Guide* also contains incorrect information about the “View page in” field.

Table 2 describes the “View page in” user configuration setting.

Table 2 **User Configuration Settings**

Field	Description
View page in	<p>From the drop-down selection box, choose the language for the User Configuration window; this changes the language that displays only for the current session.</p> <p>Note When you next log on, the User Configuration window displays in the default language. To choose the language that you want to use, download and install the appropriate Locale Installer.</p>

Using Valid Characters in Cisco CallManager User IDs

The “Add A New User” chapter in the *Cisco CallManager Administration Guide* and the Cisco CallManager online help documentation contain incorrect information about the use of special characters in the User ID field.

Specifically, the UserID field in the User Configuration Settings under the **User > Add a New User** menu incorrectly states that you may use special characters when you configure a Cisco CallManager user ID.

Do not use special characters, such as =, +, <, >, #, ;, \, , , “” and blank spaces. You must use alphanumeric characters only.

For more information, refer to
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef71945>.

Cisco CallManager Dialed Number Analyzer Private Phrase Requirement

The “Installing Cisco CallManager Dialed Number Analyzer” chapter in the *Cisco CallManager Dialed Number Analyzer Guide* contains incorrect information about the Private Phrase Requirement in [Step 6](#).

Procedure

- Step 1** Access Cisco CallManager and choose **Application > Install Plugins**.
The Install Plugins window displays.
- Step 2** Locate the Dialed Number Analyzer Plugin.
- Step 3** Click the executable icon for Dialed Number Analyzer Plugin to launch the InstallShield Wizard.
- Step 4** Click **Open**. The InstallShield Wizard for Cisco Dialed Number Analyzer window displays.
- Step 5** At the Welcome to the InstallShield Wizard for Cisco Dialed Number Analyzer window, click **Next**.
The Enter Private Phrase window displays.
- Step 6** In the Enter Private Phrase window, enter the private phrase for this cluster.
- Step 7** Click **Next**.
If the private phrase is incorrect, a message displays. Return to [Step 6](#). If the private phrase is correct, the Ready to Install the Program window displays.
- Step 8** At the Ready to Install the Program window, click **Install**.
- Step 9** At the InstallShield Wizard Completed window, click **Finish**.
The tool installs the Cisco Dialed Number Analyzer service on the machine.
-

Cisco CallManager Dialed Number Analyzer Service Startup Type

The “Installing Cisco CallManager Dialed Number Analyzer” chapter in the *Cisco CallManager Dialed Number Analyzer Guide* contains incorrect information about the service startup type being set to “Manual” after successful installation of DNA. The Dialed Number Analyzer service startup type actually gets set to “Automatic.”

Therefore, the text in the *Cisco CallManager Dialed Number Analyzer Guide* should include the following statement:

When installation is successful, the Dialed Number Analyzer service installs and starts. The service startup type gets set to Automatic.

Supported Number of Alphanumeric Characters in the AAR Group Name Field

The “Automated Alternate Routing Group Configuration” chapter in the *Cisco CallManager Administration Guide* and the Cisco CallManager online help documentation contain incorrect information about the number of alphanumeric characters that the AAR Group Name field can include.

Specifically, the documentation specifies that the AAR Group Name field can contain up to 50 alphanumeric characters when it can accommodate 20 alphanumeric characters.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef90651>.

Default Value for the Extension Mobility Alphanumeric Userid Service Parameter

The Setting Service Parameters section in the *Cisco CallManager Features and Services Guide*, Cisco CallManager Extension Mobility chapter incorrectly states that the default value for the clusterwide service parameter, Alphanumeric Userid, specifies False. The default value should reflect True.

The following information updates Step 9 in this chapter:

Step 9)

At the Alphanumeric Userid field, choose **True** to allow the UserID to contain alphanumeric characters. Choosing False allows the UserID to contain numeric characters only.

The default value specifies True.

You must restart the Cisco Tomcat Service if you change this setting.



Note The Alphanumeric Userid parameter applies system-wide. That is, all users must have alphanumeric user IDs or all users must have numeric user IDs. You cannot have a mix of the two types of user ids.

Updated Directory Path for Music On Hold Drop Directory

The “Services” chapter in the *Cisco CallManager System Guide* and the “Music on Hold” chapter in the *Cisco CallManager Features and Services Guide* contain incorrect path information about the default input directory for the Music on Hold drop directory. The correct path for the MOH audio source files should reflect:

```
c:\Program Files\Cisco\MOH\DropMOHAudioSourceFilesHere
```

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef56629>

Default Value for Display IE and Redirecting IE Delivery Fields

The “Trunk Configuration” chapter and the “Gateway Configuration” chapter in the *Cisco CallManager Administration Guide* incorrectly display “unchecked” as the default value for the check boxes used by the following fields:

- Display IE Delivery
- Redirecting IE Delivery - Inbound
- Redirecting IE Delivery - Outbound

The correct default value should specify “checked” for these fields.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef96910>

and

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef96929>

Support for Overlap Route Patterns

Cisco CallManager does not support the use of overlap route patterns with MGCP gateways that are configured with FXO ports. The “Route Pattern Configuration” chapter and the “Gateway Configuration” chapter in the *Cisco CallManager Administration Guide* do not contain this information.

Cisco CallManager continues to support overlap route patterns for BRI and PRI MGCP-controlled digital interfaces.

Changes

This section contains changes that have occurred since the original release of the *Cisco CallManager Administration Guide* release 3.3. These changes do not currently appear in the release 3.3 *Cisco CallManager Administration Guide* or the online help for the Cisco CallManager application.

- [Cisco CallManager Attendant Console, page 56](#)
- [Calling Search Space, page 57](#)
- [Custom Phone Rings, page 57](#)
- [Adding and Deleting Users by Using Cisco CallManager Administration, page 57](#)
- [Associating H.323 Devices to Users, page 58](#)
- [Changes to Gateway Support with Cisco CallManager, page 59](#)
- [Specifying Options that Display on the User Options Window, page 59](#)
- [Ad Hoc Conference Limitations, page 61](#)
- [Meet-Me Conference Limitations, page 61](#)

Cisco CallManager Attendant Console

The name Cisco CallManager Attendant Console now appears as Cisco CM Attendant Console on the drop-down menu items under Service in Cisco CallManager Administration. The menu items for Cisco CallManager Attendant Console User and Cisco CallManager Attendant Console Server now appear as Cisco CM Attendant Console User and Cisco CM Attendant Console Server.

Cisco CallManager Attendant Console supports Cisco IP Phone models 7902, 7905, 7912, 7940, 7960, and 7970. The *Cisco CallManager System Guide* only reflects support for Cisco IP Phone models 7960/7940.

Calling Search Space

When you update a Calling Search Space in Cisco CallManager Administration, you do not have to restart the devices for the changes to take effect.



Note

If you choose to restart the devices, be aware that calls on the affected gateways drop.

Custom Phone Rings

The “Custom Phone Rings” chapter now exists in the *Cisco CallManager Features and Services Guide*.

Adding and Deleting Users by Using Cisco CallManager Administration

The *Installing the Cisco Customer Directory Configuration Plugin for Cisco CallManager Release 3.3* does not contain all of the steps that are now required for adding and deleting users by using Cisco CallManager Administration. The following information provides an update to this procedure.

Procedure

Step 1 Browse to C:\dcsvr\config and open the file **UMDirectoryConfiguration.ini** in Notepad.



Note You must open the file in Notepad. Opening the file in another text editor application may corrupt the file.

Step 2 In the UMDirectoryConfiguration.ini file, locate the key **UserDirAccess**.

Step 3 Change the UserDirectAccess value to **true**.

Step 4 In Notepad, choose **File > Save** to save the file.

- Step 5** Close the UMDirectoryConfiguration.ini file.
- Step 6** Choose **Start > Run**.
- Step 7** Enter **regedit** in the Open field and click OK.
- Step 8** Browse to **\\HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\Directory Configuration** within the registry.
- Step 9** In the right pane, double-click the **DirAccess** registry key.
- Step 10** Delete the false registry entry and enter **true** as the new registry entry.
- Step 11** Restart the IIS Admin Service and its dependent services by choosing **Start > Programs > Administrative Tools> Services**.
- Step 12** Right-click IIS Admin Service and then choose **Restart**.
A dialog box prompts you to restart dependent services. These services may differ depending on your configuration.
- Step 13** Click **Yes**.
- Step 14** Restart the dependent services.
You may now add, update, or delete users within Cisco CallManager Administration. Refer to the latest version of the *Cisco CallManager Administration Guide* for information about how to perform these tasks.
-

Associating H.323 Devices to Users

In Cisco CallManager release 4.0, administrators could not associate H.323 devices with a user; therefore, the administrator could not configure features on the H.323 endpoints in the Cisco CallManager Administration User Configuration window.

Cisco CallManager release 3.3(5) corrects this behavior by displaying all devices, in addition to CTI-controllable devices, and by allowing the administrator to choose H.323 devices in the Device Association window.

For devices that are not CTI-controllable, such as H.323 devices, an asterisk (*) displays next to the device icon. All device association behavior remains identical regardless of the type of device for which the feature is configured.

Changes to Gateway Support with Cisco CallManager

Support exists for the following gateway types with Cisco CallManager release 3.3(5):

Cisco 1880

The “Gateway Configuration” chapter in the *Cisco CallManager Administration Guide* and the “Understanding Cisco CallManager Voice Gateways” chapter in the *Cisco CallManager System Guide* incorrectly list the Cisco 1880 router as a supported Cisco IOS MGCP gateway for use with Cisco CallManager. Cisco no longer supports the Cisco 1880 router for use with Cisco CallManager.

Cisco 1750, Cisco 1751, Cisco 1760

The “Understanding Cisco CallManager Voice Gateways” chapter in the *Cisco CallManager System Guide* incorrectly lists the Cisco 1750 router as a supported Cisco IOS H.323 gateway for use with Cisco CallManager. The Cisco 1751 router and the Cisco 1760 router replace the Cisco 1750 router. Cisco no longer supports the Cisco 1750 router for use with Cisco CallManager.

Cisco 2801

Cisco CallManager adds support for the Cisco 2801 router as a Cisco IOS MGCP gateway that is configurable for use with Cisco CallManager release 3.3(5).

Specifying Options that Display on the User Options Window

Cisco CallManager 3.3(5) adds support for Administrator configuration of the CCMUser Parameters in the Cisco CallManager Administration Enterprise Parameters Configuration window. These parameters allow the Administrator to configure the appropriate enterprise parameter settings in Cisco CallManager Administration to enable or disable the options that display to phone users on the Cisco CallManager User Options window.

From the Cisco CallManager User Options window, users can customize and control phone features and settings. (For detailed information about the Cisco CallManager User Options, refer to *Customizing Your Cisco IP Phone on the Web*.)

**Note**

All options that display on the Cisco CallManager User Options window can be controlled by the Administrator from the Cisco CallManager Administration Enterprise Parameters Configuration window. (By default, all options display on the Cisco CallManager User Options window until the Administrator disables options.) The settings that you make are clusterwide; that is, they affect all User Options windows at your site, and they become visible to the phone users after the next user login to the Cisco CallManager User Options window.

The following values may be configured by the Administrator for the CCMUser Parameters:

- Show Ring Settings—True or False; the default value specifies False.
- Show Call Forwarding—True or False; the default value specifies True.
- Show Speed Dial Settings—True or False; the default value specifies True.
- Show Cisco IP Phone Services Settings—True or False; the default value specifies True.
- Show Personal Address Book Settings—True or False; the default value specifies True.
- Show Message Waiting Lamp Policy Settings—True or False; the default value specifies True.
- Show Line Text Label Settings—True or False; the default specifies False.
- Show Locale for Phone Settings—True or False; the default value specifies True.
- Show Locale for Web Pages Settings—True or False; the default value specifies True.
- Show Change Password Option—True or False; the default value specifies True.
- Show Change PIN Option—True or False; the default value specifies True.
- Show Download Plugin Option—True or False; the default specifies True.
- Show Online Guide Option—True or False; the default value specifies True.

Perform the following procedure to configure the options that appear on the Cisco CallManager User Options window.

Procedure

- Step 1** From Cisco CallManager Administration, choose **System > Enterprise Parameters**.
- The Enterprise Parameters Configuration window displays.
- Step 2** In the CCMUser Parameters area, specify whether a parameter displays on the User Options window by choosing one of the following values from the Parameter Value drop-down list for each parameter:
- True—Set this option to enable display on the User Options window.
 - False—Set this option to disable display on the User Options window.
- Step 3** Click **Update** to save your settings.
-

For more information, refer to the latest version of the *Cisco CallManager Administration Guide*.

Ad Hoc Conference Limitations

Cisco CallManager supports a maximum of 100 simultaneous ad hoc conferences for each Cisco CallManager server.

Meet-Me Conference Limitations

Cisco CallManager supports a maximum of 100 simultaneous meet-me conferences for each Cisco CallManager server.

Omissions

This section lists new and additional information that the current Cisco CallManager documentation does not include:

- [New Service Parameter for Cisco CallManager Extension Mobility](#), page 62
- [H.323 Configuration Settings](#), page 63
- [Defining the Quality of Service \(QoS\) Values](#), page 65

- [Quality Report Tool Configuration Settings, page 66](#)
- [Exporting and Importing Phones with More Than One User, page 72](#)
- [Device Profile Default Configuration, page 72](#)
- [Subscribing Services to a Device Profile Default, page 77](#)
- [User Settings in Cisco CallManager Administration, page 77](#)
- [Name Change for the Cisco IAD 2400 Gateway Type in Cisco CallManager Administration, page 80](#)
- [Reinstalling Dialed Number Analyzer after a Cisco CallManager Upgrade, page 81](#)
- [Personal Directory, page 83](#)
- [Dependency Between Cisco CallManager and CTI Manager, page 88](#)
- [Using Wildcard Characters in Device Searches, page 89](#)
- [Removing a Subscriber Server from Cisco CallManager, page 89](#)

New Service Parameter for Cisco CallManager Extension Mobility

Cisco CallManager 3.3(3) introduces a new service parameter for Cisco CallManager Extension Mobility. The Cisco CallManager Extension Mobility chapter in the *Cisco CallManager Features and Services Guide* does not document this information.

At the service parameter field, Remember last user logged in, you can choose **True** to specify that the Extension Mobility application remembers the user ID of the last user that logged in to the phone. The default value for the service parameter specifies False.



Note

As with all system parameters, the setting of this system parameter applies it to all users in the Cisco CallManager cluster.

This setting proves useful in situations where individuals use their own phone on a regular basis and no one else uses that phone. For example, user may use Cisco CallManager Extension Mobility to enable the types of calls that are allowed from a phone. Individuals who are using their office phone in a logout state can make only internal or emergency calls, but after logging in using Cisco CallManager Extension Mobility, the user also can make local,

long-distance, and international calls. In this scenario, only this user regularly logs in to the phone. It makes sense to set the Extension Mobility application to remember the last user ID that is logged in.

In a true hoteling scenario, where users can come into any office and use any phone on a temporary basis, set this parameter to false.

H.323 Configuration Settings

Additions to the Phone Configuration Settings table in the Phone Configuration chapter in *Cisco CallManager Administration Guide* include the following configuration settings for H.323.

Table 3 displays these settings.

Table 3 H.323 Configuration Settings

Field	Description
H.323 Information	
Outgoing Caller ID Pattern	For incoming calls to the phone, enter the pattern, from 0 to 24 digits, that you want to use for caller ID.
Calling Party Selection	<p>Choose the directory number that is sent on an outbound call on a gateway.</p> <p>The following options specify which directory number is sent:</p> <ul style="list-style-type: none"> • Originator—Send the directory number of the calling device. • First Redirect Number—Send the directory number of the redirecting device. • Last Redirect Number—Send the directory number of the last device to redirect the call. • First Redirect Number (External)—Send the external directory number of the redirecting device. • Last Redirect Number (External)—Send the external directory number of the last device to redirect the call.

Table 3 **H.323 Configuration Settings (continued)**

Field	Description
Calling Party Presentation	<p>Choose whether the Cisco CallManager transmits or blocks caller ID.</p> <p>Choose Allowed if you want the Cisco CallManager to send caller ID.</p> <p>Choose Restricted if you do not want the Cisco CallManager to send caller ID.</p>
Display IE Delivery	<p>Check this check box to enable delivery of the display information element (IE) in SETUP and CONNECT messages for the calling and called party name delivery service.</p> <p>The default setting checks this check box.</p>
Redirecting Number IE Delivery - Outbound	<p>Check this check box to include the Redirecting Number IE in the outgoing SETUP message from the Cisco CallManager to indicate the first redirecting number and the redirecting reason of the call when the call is forwarded.</p> <p>Uncheck the check box to exclude the first redirecting number and the redirecting reason from the outgoing SETUP message.</p> <p>You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.</p> <p>The default setting checks this check box.</p>

Table 3 **H.323 Configuration Settings (continued)**

Field	Description
Redirecting Number IE Delivery - Inbound	<p>Check this check box to accept the Redirecting Number IE in the incoming SETUP message to the Cisco CallManager.</p> <p>Uncheck the check box to exclude the Redirecting Number IE in the incoming SETUP message to the Cisco CallManager.</p> <p>You use Redirecting Number IE for voice-messaging integration only. If your configured voice-messaging system supports Redirecting Number IE, you should check the check box.</p> <p>The default setting checks this check box.</p>
Media Termination Point Required	<p>Indicate whether a media termination point (MTP) is used to implement features that H.323 does not support (such as hold and transfer).</p> <p>Check the Media Termination Point Required check box if you want to use a media termination point to implement features. Uncheck the Media Termination Point Required check box if you do not want to use a media termination point to implement features.</p> <p>Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source.</p> <p>If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.</p>

Defining the Quality of Service (QoS) Values

Because the “NA” and “Infinity” values for the QoS parameters that the Cisco CallManager Serviceability CDR Analysis and Reporting (CAR) tool uses are case-sensitive, you must enter these values exactly as shown; the system does not support other forms.

Quality Report Tool Configuration Settings

Cisco CallManager 3.3 introduces the Quality Report Tool (QRT) feature. The Cisco CallManager 3.3 release documentation does not provide specific information about configuring and using the QRT feature.

The *Cisco CallManager Features and Services Guide* for Cisco CallManager release 4.1 will include the following information about QRT:

- [QRT Overview, page 66](#)
- [User Interfaces, page 67](#)
- [Creating a Softkey Template with the QRT Softkey, page 67](#)
- [Configuring the QRT Softkey Template in Device Pool, page 68](#)
- [Adding the QRT Softkey Template in Phone Configuration, page 69](#)
- [Activating the Cisco Extended Functions Service for QRT, page 69](#)
- [Configuring Alarms and Traces for QRT, page 70](#)
- [Setting the Cisco Extended Functions Service Parameters for QRT, page 71](#)
- [Using the QRT Viewer, page 72](#)

QRT Overview

The Quality Report Tool, a voice-quality and general problem-reporting tool for Cisco IP Phones, extends to IP phones as a Windows NT service.

As a feature within the Cisco Extended Functions service, QRT automatically loads with the Cisco CallManager installation. The Cisco CallManager system administrator enables the QRT feature through the use of softkey templates.

Perform these steps after installation to enable QRT availability for users and to set up reporting capabilities:

1. Properly configure the QRT feature for Cisco IP Phone users. You can configure QRT availability for up to four different call states (Connected, Connected Transfer, Connected Conference, and On Hook).
2. From Cisco CallManager Serviceability, activate the Cisco Extended Functions service and configure alarms and traces for use with QRT.
3. Define how the QRT feature will work in your system by configuring the applicable system parameters for the Cisco Extended Functions.

4. Create, customize, and view phone problem reports by using the QRT Viewer application.

**Note**

Users with administrator privileges can configure QRT and view the reports.

User Interfaces

You can choose to enable two different user modes, depending upon the amount of information that you want users to submit:

- **Interview Mode**—In this mode, the user sees extended menu choices, which allows additional user input that is related to audio quality on the IP phone and provides the ability to report other, non-audio-related problems such as the phone rebooting or the inability to make calls.

The system supports interview mode only when the IP phone is in the Connected or On Hook call state.

- **Silent Mode**—In this mode, the user does not see extended menu choices. When the user presses the QRT softkey, the system collects streaming statistics and logs the report without additional user interaction.

The system supports silent mode only when the IP phone is in the Connected, Connected Conference, or Connected Transfer call state.

When users experience problems with their IP phones, they can invoke QRT by pressing the QRT softkey on their Cisco IP Phone to easily and accurately report voice quality and other general problems.

Creating a Softkey Template with the QRT Softkey

Perform the following procedure to create a new softkey template with the QRT softkey.

Procedure

-
- Step 1** From Cisco CallManager Administration, choose **Device > Device Settings > Softkey Template**.

The Softkey Template Configuration window displays.

- Step 2** From the Softkey Template list, or from the drop-down list box in the Create a softkey template based on field, choose the Standard User softkey template. (If you choose the first option, the Softkey Template Configuration window automatically displays with new information. Go to Step 3.)
- Step 3** Click the **Copy** button.
The Softkey Template Configuration window displays with new information.
- Step 4** In the Softkey Template Name field, enter a new name for the template; for example, QRT Standard User.
- Step 5** Click the **Insert** button.
The Softkey Template Configuration redisplay with new information.
- Step 6** To add the QRT softkey to the template, click the **Configure Softkey Layout** link.
The Softkey Layout Configuration window displays. You must add the QRT softkey to the Connected, Connected Conference, Connected Transfer, and On Hook call states.
- Step 7** To add the QRT softkey to the On Hook call state, click the **On Hook** link in the Call States field.
The Softkey Layout Configuration window redisplay with the Unselected Softkeys and Selected Softkeys lists.
- Step 8** From the Unselected Softkeys list, choose the **Quality Report Tool (QRT)** softkey and click the right arrow to move the softkey to the Selected Softkeys list.
- Step 9** To save and continue, click the **Update** button.
- Step 10** To add the QRT softkey to the Connected, Connected Conference, and Connected Transfer call states, repeat [Step 7](#) through [Step 9](#) for each individual call state.



Note Ensure that you configure the QRT softkey only for the supported call states and click the **Update** button after each entry.

Configuring the QRT Softkey Template in Device Pool

Perform the following procedure to add the QRT softkey template to the device pool.

Procedure

- Step 1** From Cisco CallManager Administration, choose **System > Device Pool**.
The Device Pool Configuration window displays.
- Step 2** Choose the Default device pool or any previously created device pool that is listed in Device Pools.
You can add the template to the default device pool if you want all users to have access to the QRT softkey, or you can create a customized device pool for QRT feature users.
- Step 3** In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box.
- Step 4** Click the **Update** button.
-

Adding the QRT Softkey Template in Phone Configuration

Perform the following procedure to add the QRT softkey template to each user phone.

Procedure

- Step 1** From Cisco CallManager Administration, choose **Device > Phone**.
The Find and List Phones window displays.
- Step 2** Find the phone to which you want to add the softkey template.
In the Softkey Template field, choose the softkey template that contains the QRT softkey from the drop-down list box.
- Step 3** Click the **Update** button.
-

Activating the Cisco Extended Functions Service for QRT

Follow this procedure to activate the Cisco Extended Functions service for use with the QRT feature.

Procedure

- Step 1** From Cisco CallManager Serviceability, choose **Tools > Service Activation**.
A list of Cisco CallManager servers displays.
 - Step 2** Click the Cisco CallManager server to choose it for activation of the Cisco Extended Functions service.
 - Step 3** Check the **Cisco Extended Functions** check box.
 - Step 4** Click **Update**.
-

Configuring Alarms and Traces for QRT

Follow this procedure to configure alarms and SDI traces through Cisco CallManager Serviceability.

Procedure

- Step 1** For alarm configuration, choose **Alarm > Configuration** from the Cisco CallManager Serviceability window.
A list of Cisco CallManager servers displays.
- Step 2** Click the Cisco CallManager server to select it for alarm configuration.
- Step 3** From the Configured Services window, click **Cisco Extended Functions**.
- Step 4** Check the **Enable Alarm** check box for both Event Viewer and SDI Trace.
- Step 5** Click **Update**.
- Step 6** For trace configuration, choose **Trace > Configuration** from the Cisco CallManager Serviceability window.
A list of Cisco CallManager servers displays.
- Step 7** Click the Cisco CallManager server to select it for trace configuration.
- Step 8** From the Configured Services window, click **Cisco Extended Functions**.
- Step 9** Check the **Cisco Extended Functions Trace Fields** check box.

Step 10 Click **Update**.

For more information, refer to the *Cisco CallManager Serviceability Administration Guide*.

Setting the Cisco Extended Functions Service Parameters for QRT

Set the Cisco Extended Functions service parameters by using Cisco CallManager Administration to access the service parameters (**Service > Service Parameters**). Choose the server where the QRT application resides and then choose the Cisco Extended Functions service.

Cisco recommends that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs you to do otherwise.

Cisco Extended Functions includes the following parameters for QRT:

- **Display extended menu choices**—Determines whether extended menu choices are presented to the user. Set this field to True to display extended menu choices (interview mode) or set this field to False to not display extended menu choices (silent mode).
Recommended default value specifies False (silent mode).
- **Streaming statistics polling duration**—Determines the duration that is used for polling streaming statistics. Set this field to -1 to poll until the call ends, set it to 0 to not poll at all, or set it to any positive value to poll for that many seconds. Polling stops when the call ends.
Recommended default value specifies -1 (poll until the call ends).
- **Streaming statistics polling frequency (seconds)**—Designates the number of seconds to wait between each poll. The value range is between 30 and 3600.
Recommended default value specifies 30.
- **Log File**—Specifies the path where the QRT report files are located. Users must have the proper privileges to access these files.
Recommended default value specifies
C:\Program Files\Cisco\QRT\QRT.xml.
- **Maximum No. of Files**—Specifies the maximum number of files before restarting the file count and overwriting old files. The value range is between 1 and 10000.

Recommended default value specifies 250.

- **Maximum No. of Lines per File**—Specifies the maximum number of lines in each file before starting the next file. The value range is between 100 and 2000.

Recommended default value specifies 2000.

Using the QRT Viewer

You can use the QRT Viewer to view the IP phone problem reports that the Quality Report Tool generates. The QRT Viewer allows you to filter, format, and view the tool-generated phone problem reports, so they provide you with the specific information that you need.

For detailed information about accessing, configuring, using, and customizing the IP phone problem reports, refer to the *Cisco CallManager Serviceability Administration Guide*.

Exporting and Importing Phones with More Than One User

When you use BAT to export phone records that have multiple users who control a phone, the export utility generates a unique phone record for each user. (The phone information remains the same, but each record has a different user ID.)

When you import the exported file that contains phones with multiple users, the first phone record inserts with the associated user. However, subsequent phone records fail to insert, even though BAT attempts to insert all records and accepts the user association to the phone. In this case, the log file for the import transaction shows that the phone insertions failed for all users except the first user who is associated with the phone.

Device Profile Default Configuration

The online help for the Cisco CallManager application does not include information about Device Profile Defaults. The following sections provide information about configuring and updating device profile defaults:

- [Device Profile Default Overview, page 73](#)
- [Adding a New Device Profile Default, page 73](#)
- [Updating Device Profile Defaults, page 74](#)

- [Deleting a Device Profile Default, page 74](#)
- [Device Profile Default Configuration Settings, page 75](#)

Device Profile Default Overview

Use the device profile default whenever a user logs on to a phone model for which no user device profile exists. To create a device profile default for each phone model that supports Cisco Extension Mobility, use the Cisco CallManager Device Profile Default Configuration window. The maximum number of device profile defaults cannot exceed the number of phone models that support Cisco CallManager Extension Mobility.

For example, a user logs on to a Cisco IP Phone model 7960 for which there is a user device profile. The user device profile for the user gets downloaded to the phone to which the user logged on. Later, the same user logs on to a Cisco IP Phone model 7940 for which no user device profile exists. In this case, the device profile default for the Cisco IP Phone model 7940 gets downloaded to the phone.

A device profile default comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include device type, user locale, phone button template, softkey template, and Cisco IP Phone services.

Adding a New Device Profile Default

The device profile default contains attributes such as device type, phone template, user locale, expansion modules, softkey template, and subscribed Cisco IP Phone services. Perform the following procedure to add a device profile default.

Procedure

-
- Step 1** Choose **Device > Device Settings > Device Profile Default**.
The Device Profile Default Configuration window displays.
 - Step 2** Click the **Add a New Device Profile Default** link.
 - Step 3** Configure each field as described in [Table 4](#).
 - Step 4** Click **Insert**.

The device profile displays in the Device Profile Default pane.

Updating Device Profile Defaults

This section describes how to update a device profile default.

Procedure

- Step 1** Choose **Device > Device Settings > Device Profile Default**.
 - Step 2** From the Device Profile Default pane, click the device profile that you want to update.

The Device Profile Default Configuration window displays the profile information of the profile that you chose.
 - Step 3** Make the desired changes to the profile as described in [Table 4](#).
 - Step 4** Click **Update**.
-

Deleting a Device Profile Default

This section describes how to delete a device profile default.

Procedure

- Step 1** Choose **Device > Device Settings > Device Profile Default**.
- Step 2** From the Device Profile Default pane, click the device profile that you want to delete.

The Device Profile Default Configuration window displays the profile information of the profile that you chose.
- Step 3** Click **Delete**.

A message displays that states that this action cannot be undone.

- Step 4** To delete the device profile default, click **OK** or, to cancel the deletion, click **Cancel**.

Device Profile Default Configuration Settings

Table 4 describes the fields that are available in the Cisco CallManager Device Profile Default Configuration window.

Table 4 **Device Profile Default Configuration Settings**

Field	Description
Device Profile Default Information	
Device Type	This field specifies the device (such as an IP phone) for which a profile gets created.
User Hold Audio Source	<p>To specify the audio source that plays when a user initiates a hold action, click the drop-down arrow and choose an audio source from the list that displays.</p> <p>If you do not choose an audio source, Cisco CallManager uses the audio source that is defined in the device pool or uses the system default if the device pool does not specify an audio source ID.</p> <p>Note You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose Service > Music On Hold.</p>

Table 4 **Device Profile Default Configuration Settings (continued)**

Field	Description
User Locale	<p>From the drop-down list box, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users.</p> <p>Cisco CallManager makes this field available only for phone models that support localization.</p> <p>Note If no user locale is specified, Cisco CallManager uses the user locale that is associated with the device pool.</p> <p>Note If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. Refer to the Cisco IP Telephony Locale Installer documentation.</p>
Phone Button Template Information	
Phone Button Template	Choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Softkey Template Information	
Softkey Template	Choose the appropriate softkey template. The softkey template determines the configuration of the softkeys on Cisco IP Phones. Leave this field blank if the device pool contains the assigned softkey template.
Expansion Module Information	
Module 1	If these fields display for the phone model, choose the 7914 14-button expansion module or none.
Module 2	If these fields display for the phone model, choose the 7914 14-button expansion module or none.

Subscribing Services to a Device Profile Default

To subscribe a service such as Cisco CallManager Extension Mobility to the device profile default, perform the following procedure:

Procedure

- Step 1** Choose **Device > Device Settings > Device Profile Default**.
- Step 2** From the Device Profile Default pane, click the device profile that you want to update.
- The Device Profile Default Configuration window displays the profile information of the profile that you chose.
- Step 3** Click the **Subscribe/Unsubscribe Services** link to add Cisco IP Phone services to this profile.
- The Subscribe Cisco IP Phone services window displays.
- Step 4** From the Select a Service drop-down list box, choose the service that you want to add to the profile.
- Step 5** Click **Continue**.
- The window displays with the service that you chose. If you want to choose a different service, click **Back** and repeat [Step 4](#).
- Step 6** If a parameter exists for the service, enter the value for the parameter. For information on the parameter, click the **Description** link.
- Step 7** Click **Subscribe**.
- The service appears in the Subscribed Services list.
-

User Settings in Cisco CallManager Administration

The *Cisco CallManager Administration Guide* does not provide information for all the user settings that display in Cisco CallManager Administration.

[Table 5](#) provides a description of the user settings.

Table 5 **User Configuration Settings**

Setting	Description
First Name	Enter the user first name.
Last Name	Enter the user last name.
UserID	Enter the user identification name. Cisco CallManager does not permit modifying the user ID after it is created.
User Password	Enter five or more alphanumeric characters for the user password.
Confirm Password	Enter the user password again.
PIN	Enter five or more numeric characters for the Personal Identification Number.
Confirm PIN	Enter the PIN again.
Telephone Number	Enter the user telephone number.
Manager UserID	Enter the name of the user manager ID. The manager name that you enter must already exist in the directory as a user.
Department	Enter the user department number.
User Locale	<p>From the drop-down list box, choose the locale that is associated with the user. The user locale identifies a set of detailed information to support users, including language and font.</p> <p>Cisco CallManager uses this locale for Extension Mobility and the Cisco IP Phone User Options. For Cisco CallManager Extension Mobility log on, the locale that is specified here takes precedence over the device and device profile settings. For Cisco CallManager Extension Mobility log off, Cisco CallManager uses the user locale that is specified in the default device profile.</p> <p>Note If you do not choose a user locale, the locale that is specified in the Cisco CallManager service parameters as Default User Locale applies.</p>

Table 5 **User Configuration Settings (continued)**

Setting	Description
Enable CTI Application Use	To configure users so they can use Computer Telephony Integration (CTI) applications, check the Enable CTI Application Use check box.
Call Park Retrieval Allowed	To configure users so they can retrieve parked calls, check the Call Park Retrieval Allowed check box.
Name Dialing	This field, which is required for Cisco Auto Attendant, displays after you enter the attendant name and associate Cisco Auto Attendant with Cisco CallManager.
Associated PC	This field, which is required for Cisco SoftPhone and Cisco CallManager Attendant Console users, displays after you enter the IP address or hostname for the user PCs. For Cisco SoftPhone, you enter the information in the User Configuration window in Cisco CallManager Administration. For Cisco CallManager Attendant Console, you enter the IP address/hostname after you log in to the client PC for the first time.
Primary Extension	<p>This field displays after the user is added and represents the primary directory number for the user. You choose no primary extension when you associate devices with users.</p> <p>This configuration affects the No Primary Extension and Primary Ext. settings in the Device Association window.</p>
ICD Extension	<p>This field, which displays after you have configured the agent for CRA/CRS, indicates that the device is associated with the agent user.</p> <p>This configuration affects the No ICD Extension and ICD Ext. settings in the Device Association window.</p>
Controlled Devices	This field displays after the user is added. After the device is associated, this field displays the description information (for example, the MAC address) that the user controls.

Table 5 **User Configuration Settings (continued)**

Setting	Description
Enable Authentication Proxy Rights	This field, which is required if the authentication proxy rights for a user with Cisco CallManager Extension Mobility is enabled, displays after the user is added. If authentication proxy rights is enabled, this field displays True; if disabled, this field displays False.
View page in	<p>From the drop-down list box, choose the language in which the information in the User Configuration window will display.</p> <p>Choosing an option only changes the language that displays for the current web session. The next time that you log in to Cisco CallManager Administration, the User Configuration window will display information in the default language.</p> <p>If your preferred language does not display from the drop-down list box, install the appropriate Cisco IP Telephony Locale Installer that is available on the locale installer software page on the web.</p>
Check All on Page	When you check this check box, the system automatically checks all check boxes for the devices that display in the current Device Association window.
Check All in Search	When you check this check box in the Device Association window, the system automatically checks all checks box for all devices that display after the search occurs.

Name Change for the Cisco IAD 2400 Gateway Type in Cisco CallManager Administration

In the “Add a New Gateway” window in Cisco CallManager Administration, the “Cisco IAD 2420 (end of sale product)” gateway type has replaced the Cisco IAD 2400 gateway type.

Use the Cisco IAD 2420 gateway type to add a new Cisco IAD 2420 gateway to Cisco CallManager.

**Note**

Cisco does not support the Cisco IAD 2430 gateway for use with Cisco CallManager.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef30742>.

Reinstalling Dialed Number Analyzer after a Cisco CallManager Upgrade

The *Cisco CallManager Dialed Number Analyzer Guide* does not contain the following information about reinstalling DNA after a Cisco CallManager upgrade.

If you upgrade Cisco CallManager on any server in a cluster, you must reinstall the Dialed Number Analyzer plug-in on that node in the cluster if you want the upgraded Dialed Number Analyzer version to be installed on your machine.

Follow these procedures to uninstall Dialed Number Analyzer and to reinstall the upgraded version of Dialed Number Analyzer:

Procedure to Uninstall Dialed Number Analyzer

Step 1 Uninstall Dialed Number Analyzer by accessing Add/Remove Programs, as described below:

- a. Choose **Start > Settings > Control Panel > Add/Remove Programs**.

The Add/Remove Programs dialog displays and shows a list of programs that are installed on the machine.

- b. Choose **Cisco Dialed Number Analyzer** from the list.
- c. Click **Remove**.

Alternatively, you can uninstall Dialed Number Analyzer by using the Dialed Number Analyzer Uninstall utility, as described below:

- a. Choose **Start > Programs > Dialed Number Analyzer > Uninstall Cisco Dialed Number Analyzer**.
 - b. Follow the instructions to uninstall Dialed Number Analyzer.
-

Procedure to Reinstall Dialed Number Analyzer

- Step 1** From Cisco CallManager Administration, choose **Application > Install Plugins**. The Install Plugins window displays.
- Step 2** Navigate through the list of plugins to locate the Cisco Dialed Number Analyzer Plugin.
- Step 3** Click the executable icon for the Cisco Dialed Number Analyzer Plugin to launch the InstallShield Wizard.
- Step 4** Click **Open**.
The InstallShield Wizard for the Cisco Dialed Number Analyzer window displays.
- Step 5** Click **Next** when you see the Welcome to the InstallShield Wizard for Cisco Dialed Number Analyzer window display.
The Enter Private Phrase window displays.
- Step 6** Enter the Private Password Phrase that is configured for this Cisco CallManager cluster.
- Step 7** Click **Next**.
If you enter an incorrect private password phrase, the system displays a message. Return to [Step 6](#) to re-enter the private password phrase.
When you enter the correct private password phrase, the Ready to Install the Program window displays.
- Step 8** Click **Install**.
- Step 9** Click **Finish** when you see the InstallShield Wizard Completed window.
The tool installs the Cisco Dialed Number Analyzer service on the machine.
-

**Note**

When installation is successful, the Dialed Number Analyzer service installs and starts; the service sets the startup type to Automatic.

Personal Directory

Personal Directory provides a personal address book that is stored in the Cisco CallManager LDAP directory, a Cisco IP Phone synchronizer, and two Cisco IP Phone services: Personal Address Book and Personal Fast Dials.

The Cisco CallManager documentation does not contain the following information about configuring and using Personal Directory:

- [System Requirements, page 83](#)
- [Configuring Personal Directory, page 83](#)
- [Configuring the Personal Address Book Service, page 84](#)
- [Configuring the Personal Fast Dials Service, page 85](#)
- [Downloading the Cisco IP Phone Address Book Synchronizer, page 87](#)
- [Preparing the Phone User for Personal Directory, page 88](#)

System Requirements

The system requires the following components for use with Personal Directory:

- Cisco IP Phones models 7940, 7960, 7970
- A PC that is running Cisco CallManager 3.1 or later
- A PC that is running Windows 2000
- A Microsoft IIS Server
- Microsoft Outlook and/or Outlook Express



Note

Ensure that Microsoft Outlook is set up in Internet-only mode and the Windows Address Book is configured to share entries.

Configuring Personal Directory

To configure the Personal Directory, you must configure the Personal Address Book Service and the Personal Fast Dials Service.

- [Configuring the Personal Address Book Service, page 84](#)
- [Configuring the Personal Fast Dials Service, page 85](#)

Configuring the Personal Address Book Service

You configure the Personal Address Book by adding the service to Cisco CallManager Administration and configuring the service parameters.

Follow this procedure to configure the Personal Address Book service:

Procedure

- Step 1** Choose **Feature > Cisco IP Phone Services**.
- The Cisco IP Phone Services Configuration window displays.
- Step 2** In the Service Name field, enter the name of the service that you want to display in the menu of available services on the Cisco IP Phone User Options window, for example, My Address Book.
- Step 3** In the Service Description field, enter a description of the content that the service provides; for example, Personal Directory - Personal Address Book.
- Step 4** In the Service URL field, enter the URL of the server where the application for the Personal Address Book service is located:
- `http://<CallManager hostname or IP address>/ccmpd/xmlAddressBookInput.asp`
- Step 5** Click **Insert**.
- Step 6** Click the **New** button to the right of the Parameters list box.
- The Configure Cisco IP Phone Service Parameter window displays.
- Step 7** Add each parameter as described in [Table 6](#), beginning with UserID. When it is specified, enter the parameter name exactly as it appears in the table.
- Step 8** To add the parameter, click **Insert**.
- Step 9** When you have added the last service parameter, click **Insert and Close** to insert that parameter and close the window.
- The Cisco IP Phone Services Configuration window displays.
- Step 10** Click **Update Subscriptions**.
-

Personal Address Book Service Parameter Settings

Table 6 shows the service parameter settings for the three service parameters required for the Personal Address Book service. Where indicated, use the exact parameter name.

Table 6 *Personal Address Book Service Parameter Settings*

Field	Definition	Definition	Definition
Parameter Name	UserID (Use this exact name.)	UserPIN (Use this exact name.)	PreDial
Parameter Display Name	User Identification	PIN	Outside Access code
Default Value	None	None	None
Parameter Required	Yes	Yes	No
Parameter Description	This field specifies the same user identification that is used with the Cisco IP Phone User Options window.	This field specifies the same user PIN that is used with the Cisco IP Phone User Options window.	This access code gets added as a prefix to the stored directory number to provide access to an outside line.
Parameter is a Password (mask contents)	None	None	None



Note

To mask a parameter entry such as a password, check the Parameter is a Password (mask contents) check box. The default for this parameter specifies None. The parameter gets provisioned at runtime.

Configuring the Personal Fast Dials Service

You configure Personal Fast Dials by adding the service to Cisco CallManager Administration and configuring the appropriate service parameters.

Follow this procedure to configure the Personal Fast Dials service:

Procedure

- Step 1** Choose **Feature > Cisco IP Phone Services**.
- The Cisco IP Phone Services Configuration window displays.
- Step 2** In the Service Name field, enter the name of the service you want to display in the menu of available services on the Cisco IP Phone User Options window, for example, My Fast Dials.
- Step 3** In the Service Description field, enter a description of the content that the service provides; for example, Personal Directory - Personal Fast Dials.
- Step 4** In the Service URL field, enter the URL of the server where the application for the Personal Address Book service is located:
- `http://<CallManager hostname or IP address>/ccmpd/xmlFastDials.asp`
- Step 5** Click **Insert**.
- Step 6** Click the **New** button to the right of the Parameters list box.
- The Configure Cisco IP Phone Service Parameter window displays.
- Step 7** Add each parameter as described in [Table 7](#), beginning with UserID. When specified, enter the parameter name exactly as it appears in the table.
- Step 8** To add the parameter, click **Insert**.
- Step 9** When you have added the last service parameter, click **Insert and Close** to insert that parameter and close the window.
- The Cisco IP Phone Services Configuration window displays.
- Step 10** Click **Update Subscriptions**.
-

Personal Fast Dials Service Parameter Settings

[Table 7](#) shows the service parameter settings for the three service parameters that are required for Personal Fast Dials service. Where indicated, use the exact parameter name.

Table 7 **Personal Fast Dials Service Parameter Settings**

Field	Definition	Definition	Definition
Parameter Name	UserID (Use this exact name.)	UserPIN (Use this exact name.)	PreDial
Parameter Display Name	User Identification	PIN	Outside Access code
Default Value	None	None	None
Parameter Required	Yes	Yes	No
Parameter Description	This field specifies the same user identification that is used with the Cisco IP Phone User Options window.	This field specifies the same user PIN that is used with the Cisco IP Phone User Options window.	This access code gets added as a prefix to the stored directory number to provide access to an outside line.
Parameter is a Password (mask contents)	None	None	None

Downloading the Cisco IP Phone Address Book Synchronizer

Users must install the Cisco IP Phone Address Book Synchronizer plug-in on their computers before they can use the Personal Directory.

Use the following procedure to download the Cisco IP Phone Address Book Synchronizer installation file. After you download the file, you can distribute it to the users in your network.

Procedure

-
- Step 1** Choose **Applications > Install Plugins**.
- Step 2** Choose **Cisco IP Phone Address Book Synchronizer**.
Follow the online instructions.

- Step 3** Make the installation file available to the end users to install the Cisco IP Phone Address Book Synchronizer application on their own work station.
- a. Include tabsync in the file downloads.asp to make the application available to the users.
 - b. Provide users with the following URL to download the application:
`http://<ccm>/ccmuser/downloads.asp`
-

Preparing the Phone User for Personal Directory

After you have added the Personal Directory services and configured the service parameters, provide the phone user with the following information:

- Notification of the feature's availability
- Access to the installation file for the Cisco IP Phone Address Book Synchronizer for users to install on their own work stations
- Their user ID and PIN, if they do not already have it
- The URL for the Cisco IP Phone User Options web page for the user, if they do not already have it
- Information on using the Personal Directory services. Direct them to the *Customizing Your Cisco IP Phone on the Web*.

Dependency Between Cisco CallManager and CTI Manager

The *Cisco CallManager Serviceability System Guide* does not include the following information about the dependency between Cisco CallManager and CTI Manager.

In a Cisco CallManager cluster, both the Cisco CallManager service and CTI Manager must be activated for the system to function properly. If CTI Manager is activated and the Cisco CallManager service is deactivated, CTI Manager does not start or it terminates unexpectedly.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef89601>.

Using Wildcard Characters in Device Searches

The Cisco IP Phones chapter in the *Cisco CallManager System Guide* does not document the following information about using wildcard characters in device searches.

Cisco CallManager only supports SQL wildcards for device searches in the Cisco CallManager Administration Find and List Phones window. Therefore, you can perform a wildcard search for phones by using the percent sign (%) character, which matches any string of characters.

For example, if the Cisco CallManager database contains device names SEP1234 and SEP5678, you can query for all devices that include SEP by using the wildcard search SEP%. This query would return a list that includes SEP1234 and SEP5678.

Be aware that you cannot perform a wildcard search by using the asterisk (*) because the * character is not a recognized SQL wildcard.

For more information, refer to

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCed91256>.

Removing a Subscriber Server from Cisco CallManager

The following information provides the steps for removing a subscriber server from Cisco CallManager.

You can delete a subscriber server from the Cisco CallManager cluster by using the Server Configuration window in Cisco CallManager Administration. This deletion removes the server from the Cisco CallManager Administration database, but it does not delete all server dependencies.

To fully delete a server from the system, you must perform the following steps:

Procedure

-
- Step 1** Remove all dependencies from the server; for example, delete the Cisco CallManager service.

For additional information, refer to the *Cisco CallManager Administration Guide*, Deleting a Server chapter.

**Tip**

To view the dependencies, click the **Dependency Records** link on the Server Configuration window. For more information about Dependency Records, refer to the *Cisco CallManager Administration Guide*, Appendix A.

Step 2 Deactivate the services from the server.

Refer to the *Cisco CallManager Serviceability Administration Guide*, Service Activation chapter, for more information.

Step 3 Remove the server from Cisco CallManager Administration.

Refer to the *Cisco CallManager Administration Guide*, Deleting a Server chapter, for more information.

Step 4 If the Cisco CallManager cluster is integrated with the local DC Directory, run the command file from the command prompt that removes the DCD replication agreements from the publisher server.

See the [“Remove Redundant DCD Replication Agreements” section on page 90](#) for more information.

Remove Redundant DCD Replication Agreements

After you remove the subscriber server from the cluster, you must clean the DCD replication information from the publisher DCD by running the Clean_publisher command file. (This command file only executes on the publisher server.)

You can access this command file on servers that are running Cisco CallManager release 3.3 and later. Cisco CallManager installs the Clean_publisher command file on the server during installation of the Cisco Directory component.

To clean the DCD replication information, enter the following command from any directory on the publisher server:

```
c:\Clean_publisher.cmd
```

**Note**

If you remove the server without running the Clean_publisher.cmd command file and then add the server back with the same host name into the same cluster from where it was removed, the DCD script that is used to configure the subscriber

DCD will clean up the previous DCD replication agreement from the publisher DCD database during the Directory installation of the Cisco CallManager installation on the server.

Using Script Files to Remove a Subscriber Server from Cisco CallManager

To remove a subscriber server from Cisco CallManager, see the [“Removing a Subscriber Server from Cisco CallManager”](#) section on page 89.

If your attempts to remove a server were not successful, perform the following steps:

Procedure

- Step 1** Run the script file that cleans up subscriber-related database records and removes the SQL replication information from the publisher server.
- See the [“Remove Subscriber Information”](#) section on page 91.
- Step 2** If the Cisco CallManager cluster is integrated with the local DC Directory, run the command file that removes the DCD replication agreements from the publisher.
- For more information, refer to the *Cisco CallManager Administration Guide*, Appendix A.
-

Remove Subscriber Information

If the server removal was unsuccessful, run the script file that cleans up subscriber-related database records and removes the SQL replication information. Run the script file for the publisher server and the script file for the subscriber server.

See the [“Contents of the RemovePublisher.bat Script File”](#) section on page 92 and the [“Contents of the RemoveSubscriber.bat Script File”](#) section on page 95 for more information.



Tip

Copy the script file contents from [Example 1 on page 93](#) and [Example 2 on page 95](#) to a Notepad file and save it with a .bat extension; for example, *RemovePublisher.bat* and *RemoveSubscriber.bat*.

Run RemovePublisher.bat Script on Publisher Server

Execute the RemovePublisher.bat script file from the Cisco CallManager publisher server for the cluster that contains the subscriber that you want to remove. This script runs from the command prompt from any directory.

**Tip**

To view the procedure that runs the script, run the script with no parameters.

From any directory on the publisher server, enter the following command:

```
<path where you saved the script>:\RemovePublisher "server" "database"  
"name_of_server_to_delete_from_database connection string"
```

To find the database connection string name, follow these steps:

Procedure

- Step 1** Navigate to **Service > Service Parameters**.
- Step 2** Choose **Cisco Database Layer Monitor**.
- Step 3** Click **Advanced**.
- Step 4** Obtain the name from the Database Connection String field:
For example, DSN=CiscoCallManager;Server=ABC2.

When you run this command from the command prompt, errors display; no separate error log file gets generated.

To view the contents of the script file, see the [“Contents of the RemovePublisher.bat Script File”](#) section on page 92.

Contents of the RemovePublisher.bat Script File

[Example 1](#) displays the contents of the script file that cleans up subscriber-related database records and removes the SQL replication information from the publisher server.

Example 1 Script File Contents

```

@echo off
@if "%3x" == "x" goto Usage
echo Install stored procedure in database %2
echo USE %2
>>temp.sql
echo GO
>>temp.sql
echo DROP PROCEDURE dblRemoveServerFromDB
>>temp.sql
echo GO
>>temp.sql
echo CREATE PROCEDURE [dblRemoveServerFromDB]
>>temp.sql
echo (@servername NVARCHAR(50)) AS
>>temp.sql
echo BEGIN TRANSACTION
>>temp.sql
echo DECLARE @nodeid NVARCHAR(50), @deviceid NVARCHAR(50), @pnsid NVARCHAR(50)
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Get the Node ID'
>>temp.sql
echo SELECT @nodeid=pkid from ProcessNode where name=@servername
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete associated Device and MediaMixer'
>>temp.sql
echo WHILE (SELECT COUNT(*) FROM Device WHERE fkProcessNode=@nodeid) ^> 0
>>temp.sql
echo BEGIN
>>temp.sql
echo SELECT @deviceid=pkid from Device where fkProcessNode=@nodeid
>>temp.sql
echo PRINT 'Delete MediaMixer'
>>temp.sql
echo DELETE FROM MediaMixer WHERE fkDevice=@deviceid
>>temp.sql
echo PRINT 'Delete MOHServer'
>>temp.sql
echo DELETE FROM MOHServer WHERE fkDevice=@deviceid
>>temp.sql
echo PRINT 'Delete Device'
>>temp.sql

```

```
echo DELETE FROM Device WHERE pkid=@deviceid
>>temp.sql
echo END
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete associated CallManager records'
>>temp.sql
echo DELETE FROM CallManagerGroupMember FROM CallManagerGroupMember AS M
>>temp.sql
echo JOIN CallManager AS C ON C.pkid=M.fkCallManager WHERE C.fkProcessNode=@nodeid
>>temp.sql
echo DELETE FROM CallManager WHERE fkProcessNode=@nodeid
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete associated ProcessConfig records'
>>temp.sql
echo DELETE FROM ProcessConfig WHERE fkProcessNode=@nodeid
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete associated AlarmConfig records'
>>temp.sql
echo DELETE FROM AlarmConfig FROM AlarmConfig AS A JOIN ProcessNodeService
>>temp.sql
echo AS S ON A.fkProcessNodeService=S.pkid WHERE S.fkProcessNode=@nodeid
>>temp.sql
echo PRINT 'Delete associated ProcessNodeService records'
>>temp.sql
echo DELETE FROM ProcessNodeService WHERE fkProcessNode=@nodeid
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete associated ComponentVersion records'
>>temp.sql
echo DELETE FROM ComponentVersion WHERE fkProcessNode=@nodeid
>>temp.sql
echo --
>>temp.sql
echo PRINT 'Delete the node'
>>temp.sql
echo DELETE FROM ProcessNode WHERE pkid=@nodeid
>>temp.sql
echo --
>>temp.sql
echo COMMIT TRANSACTION
>>temp.sql
```

```

echo GO
>>temp.sql
echo -- Execute procedure on server %1
echo exec dblRemoveServerFromDB '%3'
>>temp.sql
osql -S %1 -d %2 -E -e -i temp.sql
del temp.sql
echo USE %2
>temp1.sql
echo GO
>>temp1.sql
echo sp_dropsubscription @publication = '%2', @subscriber = '%3', @article='all'
>>temp1.sql
echo GO
>>temp1.sql
osql -S %1 -d %2 -E -e -i temp1.sql
del temp1.sql
goto endd
:Usage
@echo Usage:
RemoveServerFromDB "server" "database" "name_of_server_to_delete_from_ProcessNode.Name"
@echo Example: RemoveServerFromDB . CCM0300 fred.cisco.com
:endd

```

Contents of the RemoveSubscriber.bat Script File

[Example 2](#) displays the contents of the script file that removes the SQL replication information from the subscriber server.

Example 2 *Script File Contents*

```

@echo off
@if "%2x" == "x" goto Usage
echo Install stored procedure in database %2

echo sp_removedbreplication @dbname = %2           >temp1.sql
echo GO                                           >>temp1.sql
osql -S %1 -d %2 -E -e -i temp1.sql

del temp1.sql

goto endd
:Usage
@echo Usage: RemoveSubscription "server" "database"
@echo Example: RemoveSubscription . CCM0300
:endd

```

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.